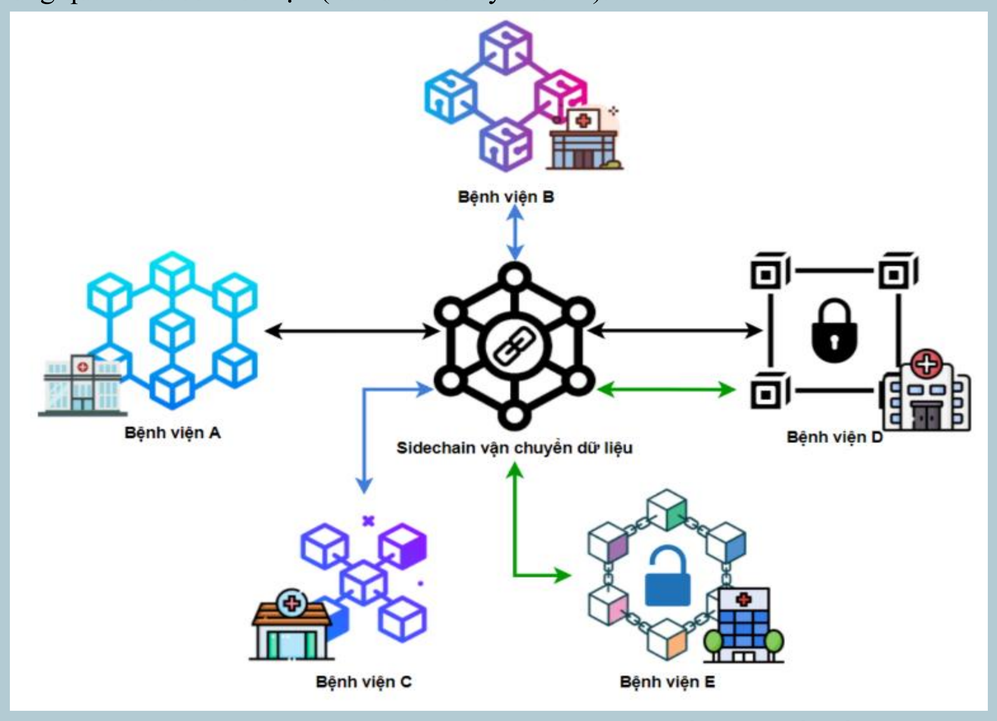
DE-SMARTHEALTHCARE - GIẢI PHÁP CHIA SẺ HỒ SƠ DỮ LIỆU Y TẾ ĐIỆN TỬ SỬ DỤNG CÔNG NGHỆ TƯƠNG TÁC LIÊN CHUỖI KHỐI

Võ Anh Kiệt, Nguyễn Bình Thục Trâm, Nguyễn Bùi Kim Ngân, Lê Trần Thùy Trang, Trần Đức Minh

Đặt vấn đề

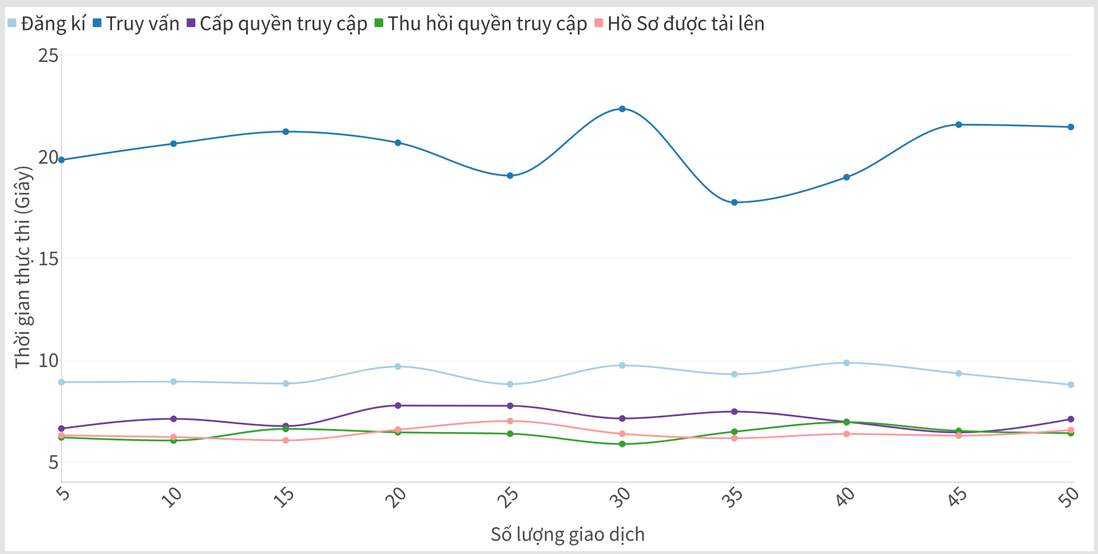
Nhiều lĩnh vực, đặc biệt là lĩnh vực chăm sóc sức khỏe đang dần chuyển từ việc quản lý dữ liệu tập trung sang quản lý dữ liệu phi tập trung bằng blockchain để có những ưu điểm vượt trội trong đảm bảo bảo mật hệ thống và quyền riêng tư của dữ liệu. Tuy nhiên, sự tồn tại của nhiều giao thức và công nghệ làm cho việc trao đổi thông tin giữa các blockchain độc lập trở nên phức tạp và không đảm bảo được tính toàn vẹn và minh bạch của dữ liệu, dẫn đến sự không tương thích và cô lập trong hệ sinh thái blockchain. Để giải quyết vấn đề này, tích hợp khả năng tương tác giữa các chuỗi khối hoặc kiến trúc chéo chuỗi là một giải pháp triển vọng. Chúng em đề xuất hướng giải quyết bằng cách xây dựng một hệ thống chuỗi khối ngoài (Sidechain). Bên cạnh đó chúng em 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).



Hình 1. Mô hình các bệnh viện với Mạng chuỗi khối được kết nối với nhau

Kết quả thực nghiệm

Hình 5 là kết quả đo thời gian của từng giao dịch với 50 lần đo để đảm bảo độ chính xác và độ tin cậy.



Hình 5. Kết quả thực nghiệm về mặt thời gian

Bảng 1 trình bày kết quả tính toán phí giao dịch cho mỗi hoạt động, được đo bằng đơn vị gas và mức sử dụng CPU.

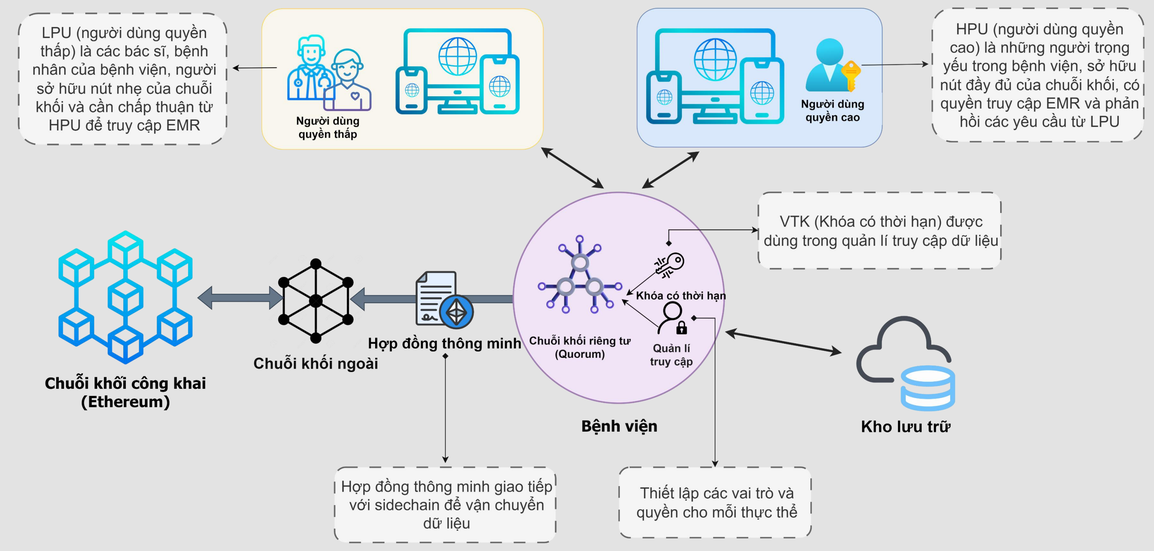
Đối tượng	Hoạt động	Mức sử dụng CPU	Phí Gas	USD
Thực thể trong Blockchain	Đăng kí người quản lý	66.29%	46407	4.46
	Đăng kí bác sĩ	66.17%	46378	4.45
	Đăng kí bệnh nhân	66.12%	46378	4.45
EMR	Lưu trữ	62.22%	92664	8.90
Điều khiển truy cập dữ liệu	Cấp quyền truy cập	66.82%	161275	15.48
	Thu hồi quyền truy cập	66.60%	30261	2.91
Bằng chứng toàn vẹn	Truy vấn	76.31%	229851	22.07

Bảng 1. Kết quả thực nghiệm về chi phí

Hoạt động truy vấn có thời gian và chi phí cao nhất. Truy vấn là giao dịch trọng tâm, thực hiện liên chuỗi do đó cần nhiều tài nguyên để hoạt động trơn tru an toàn.

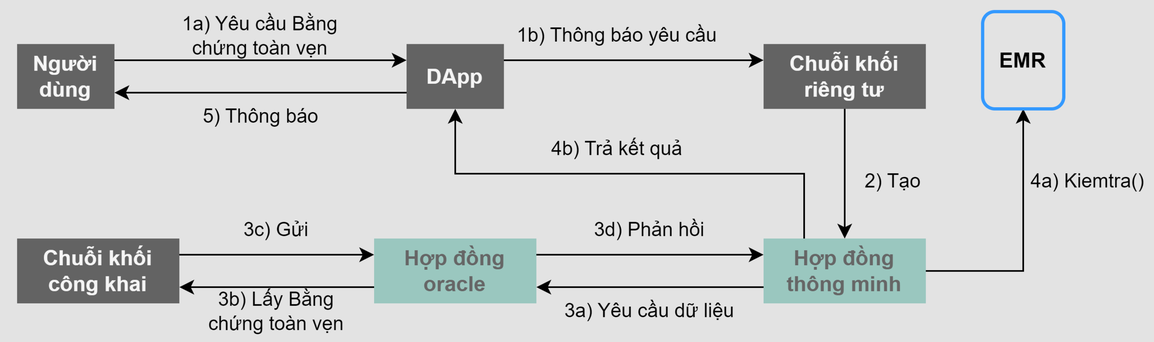
Nhìn chung, kết quả cho thấy hệ thống hoạt động hiệu quả và nhiều tiềm năng.

Kiến trúc giải pháp



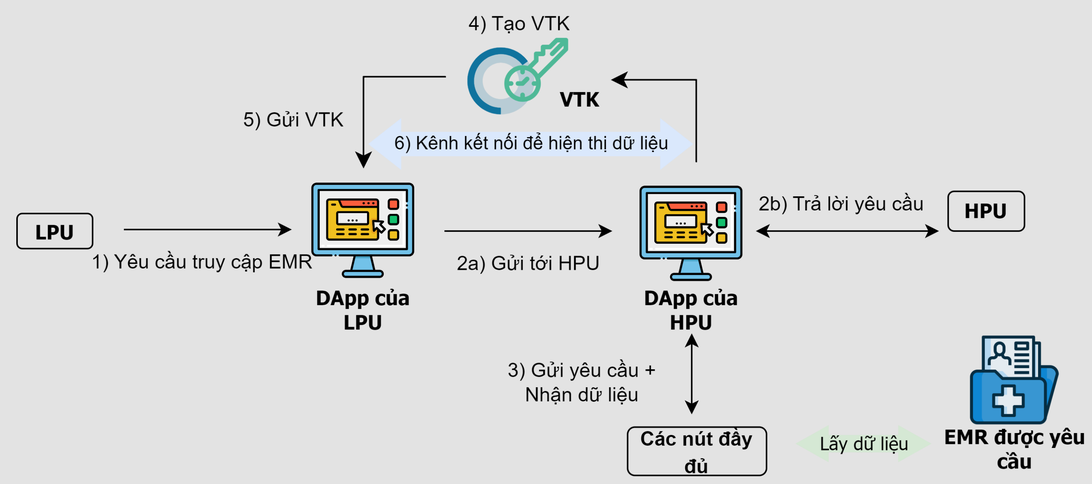
Hình 2: Mô hình tổng quan của hệ thống De-SmartHealthCare

Giải pháp chuỗi khối ngoài hoạt động như một người trung gian để vận chuyển dữ liệu giữa hai chuỗi khối không đồng nhất, với kiến trúc là mạng các Oracles phi tập trung, cho phép tiếp nhận dữ liệu từ thế giới bên ngoài vào chuỗi khối và như cũng gửi dữ liệu nội bộ ra. Oracle có nhiệm vụ bao gồm kích hoạt hợp đồng Oracle có khả năng giao tiếp được với các hợp đồng thông minh của các chuỗi khối, lấy ra hoặc cung cấp dữ liệu cho chuỗi khối. Mỗi Oracle chịu trách nhiệm cho một yêu cầu từ người dùng thông qua DApp, tiến hành truyền liên chuỗi Bằng chứng toàn vẹn để kiểm tra EMR được chỉ định.



Hình 3. Quy trình trao đổi dữ liệu liên chuỗi

Hệ thống kiểm soát truy cập dữ liệu bằng khóa có thời hạn (VTK) để cung cấp cho người dùng quyền thấp quyền truy cập EMR. Các nút đầy đủ quyết định cho yêu cầu từ người dùng, nếu chấp thuận, EMR sẽ được người dùng quyền cao giải mã bằng khóa bí mật, và một kênh kết nối tới dữ liệu được tạo. Người dùng quyền thấp được cấp một khóa đặc biệt để kết nối tới kênh này và truy cập dữ liệu cho tới hết thời gian hiệu lực của khóa.



Hình 4. Quy trình cấp quyền cho người dùng quyền thấp

Kết luận & Hướng phát triển

Trong đề tài này, chúng em đã đề xuất giải pháp tận dụng sức mạnh của chuỗi khối ngoài để tạo kết nối giữa các chuỗi khối khác nhau thông qua một mạng phi tập trung. Khóa có thời hạn được sử dụng để quản lý truy cập dữ liệu một cách an toàn và thuận tiện.

Kết quả thử nghiệm cho thấy hiệu suất và tính khả dụng của hệ thống vượt trội, đảm bảo tính bảo mật thông tin liên chuỗi. Giải pháp này có thể áp dụng trong nhiều ngành và tiếp tục nghiên cứu để nâng cao hiệu suất và bảo mật.

Trong tương lai, chúng em đặt ra mục tiêu nâng cao hiệu suất hệ thống, giảm chi phí và thực hiện các thử nghiệm rộng rãi để tận dụng toàn bộ tiềm năng của việc sử dụng dữ liệu chuỗi khối từ bên ngoài. Chúng em cũng đang tập trung vào cải thiện tính an toàn của hệ thống và tìm kiếm các phương pháp thay thế cho các hàm băm có khả năng xác minh tính toàn vẹn của dữ liệu đồng thời tương thích với chuỗi khối.