|  |  |  |  |
| --- | --- | --- | --- |
| LOGO DHCNTT -hinh.jpg | ĐẠI HỌC QUỐC GIA TP. HCM  **TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN** | Ngày nhận hồ sơ |  |
| *(Do CQ quản lý ghi)* | |

**THUYẾT MINH**

ĐỀ TÀI KHOA HỌC VÀ CÔNG NGHỆ CẤP SINH VIÊN 2023

# THÔNG TIN CHUNG

## A1. Tên đề tài

* Tên tiếng Việt: HƯỚNG TỚI KHẢ NĂNG TƯƠNG TÁC LIÊN CHUỖI KHỐI SỬ DỤNG CHUỖI KHỐI NGOÀI VÀ KIỂM SOÁT TRUY CẬP DỮ LIỆU BẰNG KHÓA CÓ THỜI HẠN
* Tên tiếng Anh: TOWARDS BLOCKCHAIN INTEROPERABILITY USING SIDECHAIN AND VALID TIME KEY-BASED DATA ACCESS CONTROL

## A2. Loại hình nghiên cứu

*(Tham khảo tiêu chuẩn đề tài đối với từng loại hình NC, chọn 01 trong 03 loại hình)*

⌧ Nghiên cứu cơ bản

□ Nghiên cứu ứng dụng

□ Nghiên cứu triển khai

## A3. Thời gian thực hiện

**..06..** tháng (kể từ khi được duyệt).

## A4. Tổng kinh phí

*(Lưu ý tính nhất quán giữa mục này và mục B8. Tổng hợp kinh phí đề nghị cấp)*

Tổng kinh phí: …**6**.. triệu đồng,gồm

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

## A5. Chủ nhiệm

Họ và tên:Võ Anh Kiệt

Ngày, tháng, năm sinh: 27/12/2002 . Giới tính (Nam/Nữ): Nam.

Số CMND: 079202029779; Ngày cấp: 21/12/2021; Nơi cấp: Cục cảnh sát

Mã số sinh viên: 20520605**.**

Số điện thoại liên lạc: 0365642317**.**

Đơn vị (Khoa hoặc BM KH&KTTT): Khoa Mạng máy tính và truyền thông**.**

## A7. Nhân lực nghiên cứu

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Họ tên** | **MSSV** | **Khoa/ Bộ Môn** |
| 1 | Võ Anh Kiệt | 20520605 | MMT&TT/ATTT |
| 2 | Nguyễn Bình Thục Trâm | 20520815 | MMT&TT/ATTT |
| 3 | Nguyễn Bùi Kim Ngân | 20520648 | MMT&TT/ATTT |

# MÔ TẢ NGHIÊN CỨU

## B1. Giới thiệu về đề tài

*(Ghi các ý về tổng quan tình hình nghiên cứu liên quan đến đề tài, lý do thực hiện đề tài, các thách thức)*

Chuỗi khối (Blockchain) là một công nghệ Sổ cái phân tán (Distributed Ledger Technology – DLT) nổi bật, nó có sẵn tính phi tập trung, minh bạch và có thể dễ dàng thực hiện kiểm toán, vì vậy các dịch vụ và giao dịch trên chuỗi khối trở nên đáng tin cậy và có tính xác thực cao hơn. Việc áp dụng chuỗi khối trong các lĩnh vực khác nhau sẽ giúp cho dịch vụ được cung cấp một cách phi tập trung, giảm thiểu độ trễ, giảm thiểu sai sót và gian lận, đồng thời cũng giúp xác minh nguồn gốc của mọi quyết định và giao dịch diễn ra trên chuỗi khối. Tuy nhiên, vì các kiến trúc chuỗi khối khác nhau thường có các yêu cầu thiết kế khác nhau, các tổ chức, doanh nghiệp hoặc nhà phát triển thường sẽ cần chọn lựa chiến trúc chuỗi khối tối ưu cho nhu cầu của mình, chẳng hạn như chuỗi khối công khai (Public blockchain), chuỗi khối riêng tư (Private blockchain), chuỗi khối tập đoàn (Consortium blockchain).[1]

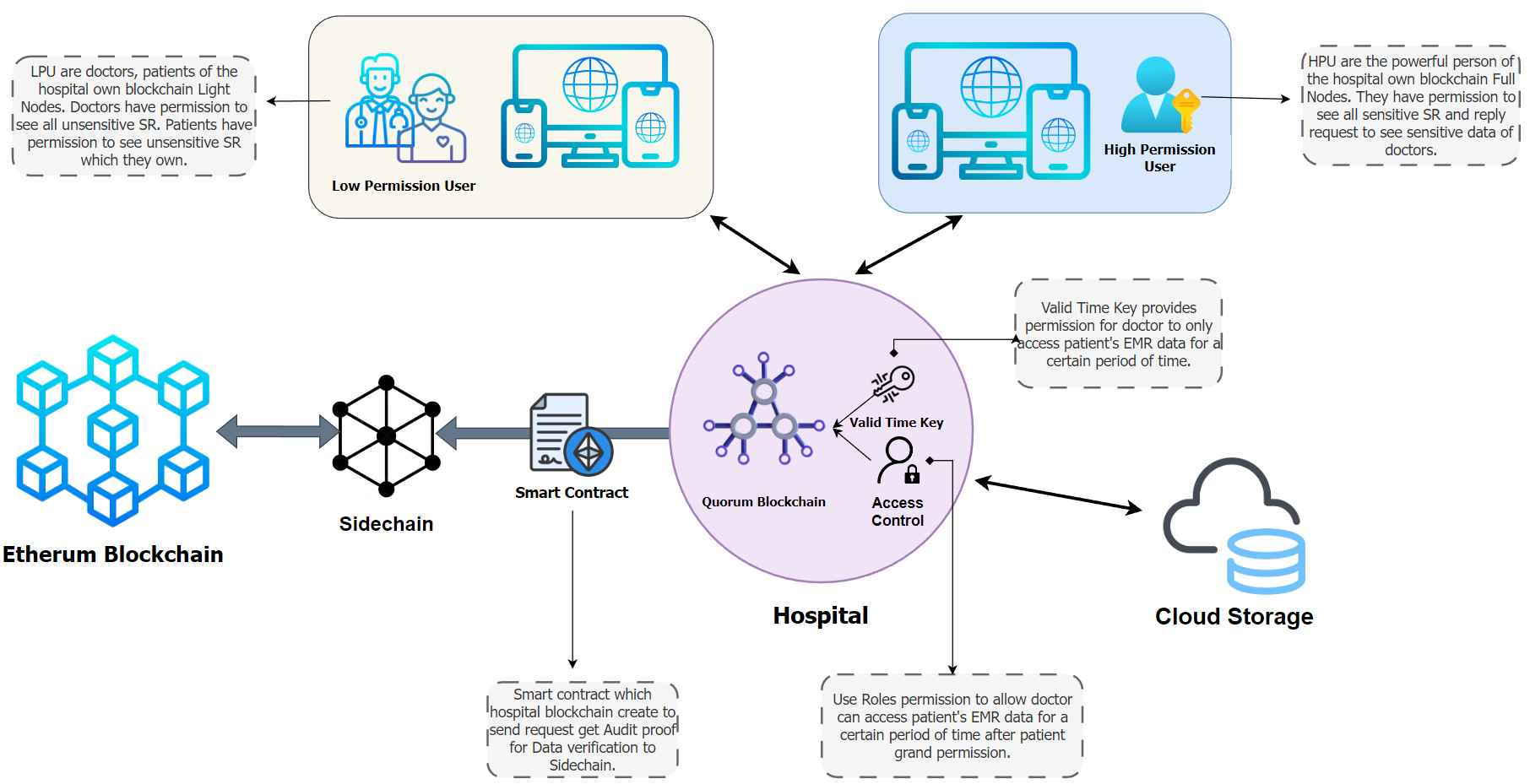
Một nghiên cứu gần đây đã cho thấy rằng [2], chuỗi khối (Blockchain) đã được áp dụng trong nhiều lĩnh vực khác nhau, bao gồm tài chính, bảo hiểm, dịch vụ lưu trú và ăn uống, chăm sóc sức khỏe và hỗ trợ xã hội. Và khá thú vị rằng, các nghiên cứu đã đưa ra những dấu hiệu cho việc khả năng tương tác giữa hai chuỗi khối đang dần trở thành mối quan tâm tiềm năng trong tương lai. Vì hiện nay, trong số các lĩnh vực đang ứng dụng chuỗi khối, có 9% là lĩnh vực liên ngành, 88% đã chia sẻ việc sử dụng mạng chuỗi khối cho các bên khác nhau và 73% đang có kế hoạch mở rộng và tăng cường hợp tác với các đối tác mới. Vì vậy, tuy rằng chuỗi khối mang lại nhiều lợi ích như đã được đề cập trước đó, thế nhưng công nghệ này lại thiếu khả năng tương tác với nhau [3,4,5]. Chính vì thế, khả năng tương tác liên chuỗi sẽ giúp đẩy mạnh quá trình phát triển của chuỗi khối trong tương lai.

Nếu chỉ xét riêng trong lĩnh vực y tế, hệ sinh thái chăm sóc sức khỏe rộng lớn bao gồm một số bên liên quan được kết nối với nhau bởi các nhu cầu hoặc các mục đích cạnh tranh khác nhau. Môi trường chăm sóc sức khỏe có rất cần có mức độ trao đổi toàn diện và đáng tin cậy ở cao giữa các bên liên quan.[6] Tuy nhiên, đối với các hệ thống chuỗi khối thì các thông tin được lưu trữ phân mảnh và phân tán trong nhiều hệ thống lưu trữ khác biệt, vì vậy dẫn đến không có đầy đủ thông tin được đảm bảo mức độ tin cậy để sử dụng trong quá trình chăm sóc và đưa ra điều kiện. Điều này xảy ra do mỗi trung tâm y tế quản lý thông tin y tế theo cách cô lập và tập trung với các kiến trúc hệ thống lưu trữ và kiểm soát khác nhau, dẫn đến quá trình trao đổi thông tin giữa các bên liên quan trở nên phức tạp và khó kiểm soát. Tương tự như vậy, quản lý thông tin tập trung cũng dẫn đến nhiều rủi ro về an toàn thông tin. Đây là điều được nhấn mạnh bởi [7], trong đó đề cập rằng chăm sóc sức khỏe là một trong những lĩnh vực dễ bị tấn công mạng nhất. Các cuộc tấn công từ chối dịch vụ (DoS) có thể xảy ra dẫn đến mất thông tin, hoặc một cuộc tấn công bằng mã độc tống tiền để chiếm đoạt thông tin mà trong nhiều trường hợp không thể phục hồi được [8]. Vì những lý do này hay những lý do khác, cần phải có các cơ chế góp phần đạt được khả năng tương tác giữa các hệ thống thông tin hỗ trợ các quy trình quản lý và chăm sóc người bệnh của các cơ sở y tế [9]. Ngoài ra, bảo mật là một yếu tố không thể thiếu đối với hồ sơ của bệnh nhân, vì nhiệm vụ này kéo theo nhiều rủi ro gây thiệt hại nghiêm trọng cho danh tiếng, bảo hiểm và tài chính,...

Chính vì vậy, nhu cầu về một hệ thống hỗ trợ tương tác liên chuỗi phục vụ cho quá trình xác minh thông tin là vô cùng cấp thiết và mang lại nhiều tiềm năng. Đã có một số nghiên cứu liên quan đến vấn đề này, chẳng hạn như [10], nhóm tác giả đã đề xuất hệ thống mang tên BeDVC thực hiện xác minh dữ liệu trao đổi giữa hai chuỗi khối mà không để lộ thông tin từ 2 blockchain. Hay như trong bài báo [11], nhóm tác giả sử dụng ứng dụng phi tập trung như một tầng phiên dịch có khả năng giao tiếp giữa nhiều blockchain, từ đó xử lí các yêu cầu trao đổi dữ liệu trên 2 blockchain khác nhau. Tuy nhiên các giải pháp này thường rất đắt đỏ và quy trình phức tạp, gặp nhiều khó khăn khi ứng dụng vào thực tiễn.

Hướng tiếp cập khác để giải quyết vấn đề trao đổi dữ liệu ngoài chuỗi là dùng Blockchain oracle. Trong [12], để giải quyết bài toán xác minh một giao dịch có trong blockchain không, tác giả đưa ra cơ chế tổng hợp và xác minh bằng oracles nodes, tuy nhiên mô hình này không thích hợp cho trao đổi dữ liệu.

Để vượt qua các khó khăn trên và giải quyết các nhược điểm còn tồn tại trong các hệ thống tương tác liên chuỗi trước đó, trong đề tài nghiên cứu này, chúng tôi hướng đến một hệ thống cung cấp khả năng tương tác và chia sẻ dữ liệu liên chuỗi sử dụng chuỗi ngoài (Sidechain) có cơ chế kiểm soát truy cập dữ liệu bằng khóa có thời hạn (VTK) để phục vụ quá trình xác minh dữ liệu (Data verification) chuỗi khối.



*Hình 1: Mô hình tổng quan*

Ngữ cảnh chúng tôi đưa ra là bệnh viện sử dụng hệ thống lưu trữ trên cloud kết hợp với private blockchain để lưu và quản lí thông tin các ca mổ diễn ra trong bệnh viện. Trong ngữ cảnh này, blockchain đóng vai trò quan trọng vì nó có thể cung cấp khả năng cập nhật lịch sử ca mổ theo thời gian thực ngay sau khi các ca mổ hoàn thành, đồng thời bảo đảm thông tin ca mổ sẽ được đảm bảo tính toàn vẹn khi đã được lưu lên blockchain. Mặt khác, hệ thống private blockchain cũng mang tính thuận tiện cao trong quá trình sử dụng thông tin khi tất cả các nodes đều có thể truy cập và xem dữ liệu, đồng thời đảm bảo tính bảo mật một số thông tin nhạy cảm thông qua phân quyền nodes của private blockchain và sử dụng khóa có thời hạn (VTK). Và cuối cùng là, trước khi lịch sử ca mổ được đưa lên hệ thống thường cần có sự xác nhận của những bên liên quan (chẳng hạn như bác sĩ chính, trưởng khoa,…) vậy nên nếu như sử dụng blockchain, quá trình này sẽ chính là cơ chế đồng thuận trước khi các dữ liệu được đưa lên blockchain, đảm bảo tính xác thực của thông tin.

Có thể thấy, hệ thống blockchain có nhiều ưu điểm phù hợp với việc lưu trữ và quản lí lịch mổ cho bệnh viện, tuy nhiên, hệ thống này lại có một điểm yếu chí mạng là chi phí xây dựng. Hiện nay, chi phí để xây một hệ thống private blockchain với tất cả các node đều có quyền vote trong cơ chế đồng thuận và lưu trữ toàn bộ thông tin trong mạng (Full node) là rất cao, nhưng nếu xây dựng một hệ thống quá ít full node và kết hợp với nhiều light node (Các node chỉ có quyền lưu trữ thông tin không nhạy cảm, không có quyền vote trong cơ chế đồng thuận) thì sẽ rất dễ bị tấn công mạng do bị mất đi tính phi tập trung. Vậy nên, câu hỏi đặt ra là làm cách nào để tối ưu chi phí nhưng vẫn đảm bảo được tính phi tập trung cần thiết trong private blockchain? Ở đây, chúng ta có một giải pháp được đưa ra bởi [12] có thể giải quyết vấn đề này bằng cách đưa các dữ liệu xác thực thông tin quan trọng lên một hệ thống public blockchain nhằm tăng tính phi tập trung và mỗi khi sử dụng sẽ gọi các dữ liệu này về để xác thực thông tin trước khi đưa lên blockchain nội bộ. Để hiện thực hóa giải pháp này thì hai blockchain cần có khả năng trao đổi dữ liệu qua lại với nhau, nhưng như đã trình bày trước đó, quá trình giao tiếp liên chuỗi hiện tại vẫn còn rất phức tạp và khó khăn, vì vậy trong bài báo này, chúng tôi đề xuất một hệ thống giao tiếp liên chuỗi khối thông qua blockchain ngoài (sidechain) sử dụng khóa có thời hạn để quản lí truy cập dữ liệu.

Cụ thể về mặt kĩ thuật sẽ như sau:

Trong kiến trúc, chúng tôi xây dựng một sidechain kiến trúc oracle phi tập trung đóng vai trò trung gian để kết nối smart contracts của blockchain với dữ liệu ngoài chuỗi. Oracle nodes sử dụng giao thức Cross-Chain Interoperability Protocol (CCIP) khi giao tiếp trực tiếp với blockchain. Blockchain B tạo smart contracts B, gửi request đến oracle node rằng cần lấy dữ liệu từ blockchain A. Oracle node nhận yêu cầu, kết nối tới blockchain A. Blockchain A tạo smart contracts A, đưa dữ liệu cần tìm cho oracle node. Oracle node nhận kết quả và trả về cho blockchain B.

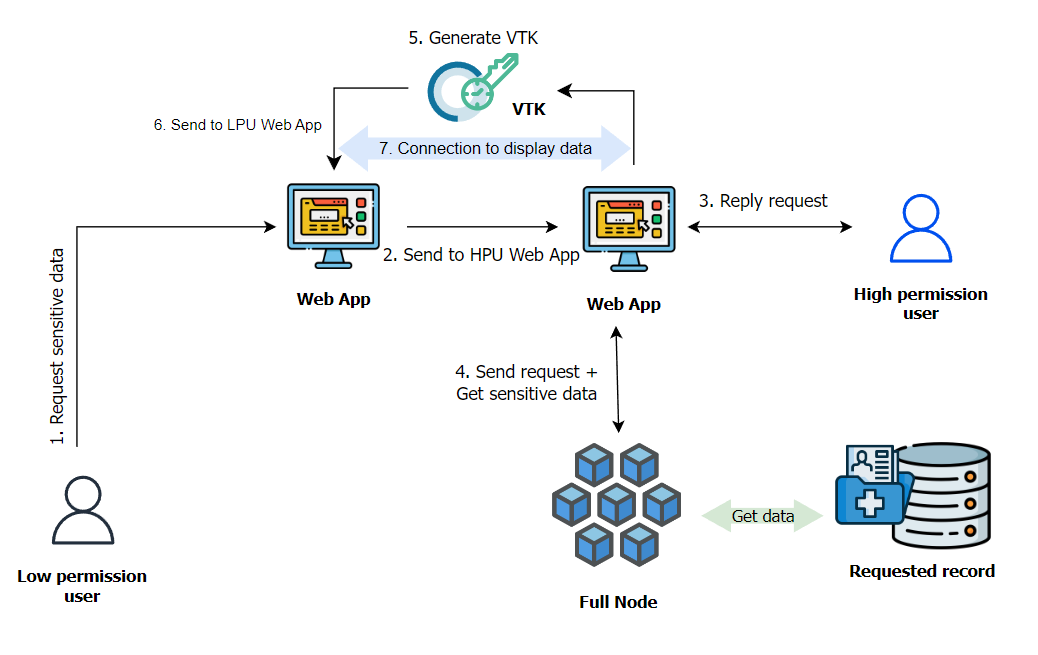
A picture containing diagram

Description automatically generated

*Hình 2. Cách hoạt động của Cross-chain Oracle*

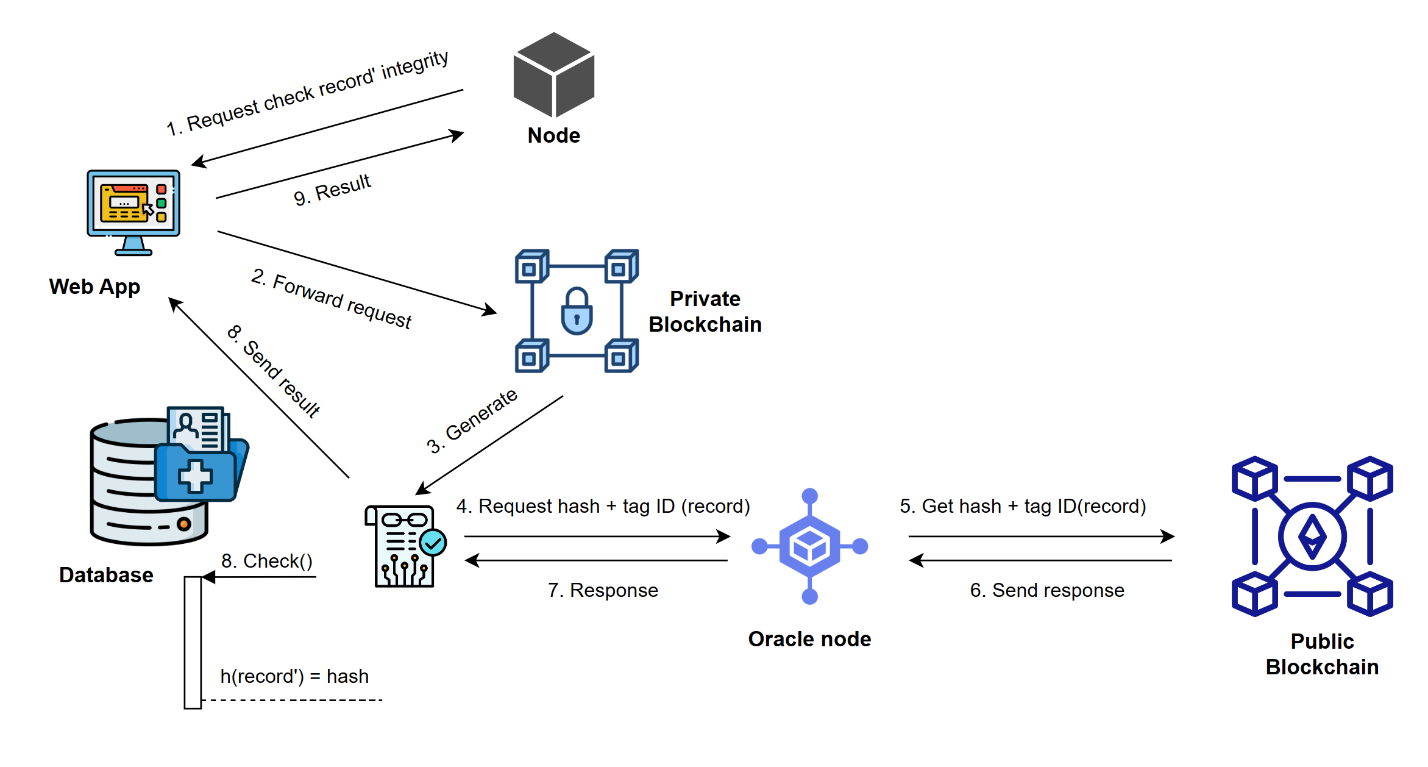
Tiếp theo, nhằm mục đích bảo mật và an toàn thông tin; tối ưu quy trình yêu cầu chia sẻ và phục vụ cho việc ứng dụng trong thực tế, chúng tôi thiết kế phân quyền truy cập trong private blockchain. Hệ thống private blockchain Quorum cung cấp tính năng hỗ trợ phân quyền truy cập để kiểm soát quyền truy cập vào dữ liệu và chức năng blockchain. Vì vậy, Smart Contract phân quyền truy cập có thể được cấp cho các tài khoản hoặc nhóm tài khoản sẽ được thêm trực tiếp vào các tệp cấu hình được sử dụng để cấu hình node Quorum. Cụ thể, cá nhóm tài khoản và quyền của nhóm sẽ được chia thành ba vai trò chính: Bác sĩ/Nhân viên y tế/Bệnh nhân liên quan – Người dùng quyền thấp: Là các light node có thể đọc và chỉnh sửa những nội dung không nhạy cảm, trong một số trường hợp có thể xem và chỉnh sửa nội dung nhạy cảm nếu được full node cấp VTK để truy cập vào dữ liệu; Trưởng khoa/Người quản lí – Người dùng quyền cao: Là các full node đóng vai trò xác nhận thông tin ca mổ, có thể đọc và chỉnh sửa các nội dung nhạy cảm, có khả năng cấp VTK cho light node khi được yêu cầu; Admin: Được cấp tất cả quyền, là người quản lý toàn hệ thống và giải quyết những trường hợp khẩn cấp.

Trong đó, khóa có thời hạn sẽ được sử dụng trong trường hợp các người dùng quyền thấp có nhu cầu đọc hoặc chỉnh sửa dữ liệu nhạy cảm đã được lưu dưới dạng mã hóa trong database. Khi đó, light node sẽ gửi yêu cầu đến full node, nếu người dùng quyền cao chấp thuận yêu cầu, full node sẽ sử dụng private key để giải mã nội dung nhạy cảm, sau đó mở một kết nối và tạo ra VTK gửi đến web app của light node. Web app sẽ dùng VTK này để kết nối vào để có thể đọc nội dung dữ liệu. Sau khi hết thời hạn key, full node sẽ lập tức đóng kết nối và light node không còn có thể đọc được dữ liệu nhạy cảm nữa. Mô hình về quy trình chi tiết này chúng tôi đã thể hiện qua *Hình 3*.

******

*Hình 3. Quy trình yêu cầu dữ liệu nhạy cảm từ người dùng quyền thấp*

Tiếp theo, toàn bộ quy trình trao đổi dữ liệu để xác thực thông tin giữa private blockchain và public blockchain chúng tôi đề xuất sẽ giống như *Hình 4* bên dưới*.*Đầu tiên, khi cần phải xác thực tính toàn vẹn thông tin của các dữ liệu đang được lưu trữ trong hệ thông, người dùng quyền cao (người dùng full node) sẽ sử dụng web app để gửi yêu cầu xác thực này cho private blockchain, một smart contract để giao tiếp với oracle node của side chain để để yêu cầu audit proof từ public blockchain. Audit proof này sẽ bao gồm record lưu thông tin ca mổ và tag ID của record đã được lưu trên public blockchain từ trước. Tiếp theo, oracle sẽ trực tiếp giao tiếp với public blockchain và lấy audit proof về cho private blockchain để private blockchain thực hiện xác thực tính toàn vẹn của dữ liệu. Sau khi hoàn thành, kết quả của quá trình xác minh sẽ được trả về và hiển thị cho người dùng thông qua web app.

*Hình 4. Quy trình vận chuyển thông tin xác minh dữ liệu giữa private blockchain và public blockchain.*

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

### B2.1 Mục tiêu

* Thực hiện cải tiến việc phân quyền truy cập và kiểm soát truy cập ở mạng blockchain Private Quorum Blockchain.
* Cải tiến mô hình trao đổi bằng chứng để xác minh dữ liệu giữa Public Etherum Blockchain và Private Quorum Blockchain để giảm chi phí.
* Sử dụng việc kiểm soát truy cập dữ liệu ở mạng blockchain Ethereum thông qua Valid Time Key

### B2.2 Nội dung và phương pháp nghiên cứu

**Nội dung 1: Tìm hiểu kiến trúc, quy tắc hoạt động, phân quyền truy cập, quản lý dữ liệu bằng khóa có thời hạn (Valid Time Key – VTK) trong mạng Blockchain (Etherum, Quorum và các loại blockchain khác).**

* Mục tiêu:
  + Nắm vững kiến thức về Solidity, tổng quan về kiến trúc và các đặc điểm. Hiểu về các thành phần, cách hoạt động và các thư viện hỗ trợ.
  + Nắm được kiến trúc, quy tắc hoạt động của mạng Public Blockchain, Private Blockchain và triển khai hệ thống mạng Etherum Public Blockchain và Quorum Private Blockchain.
  + Triển khai tính năng phân quyền bằng Smart Contract và đưa vào sử dụng trong mạng Quorum Blockchain.
  + Nắm được kiến thức về VTK, cách tạo và cách hoạt động trong hệ thống.
  + Xây dựng Smart Contract có tính năng tạo và phân phát VTK trong mô hình mạng Private Blockchain và sử dụng VTK để kiểm soát truy cập dữ liệu trong mô hình Blockchain.
* Phương pháp:
  + Tham khảo các mô hình Blockchain để lựa chọn và xây dựng một mô hình Blockchain tối ưu.
  + Nghiên cứu tài liệu và video hướng dẫn, để thực hiện triển khai mạng Blockchain.
  + Tham khảo các bài báo nghiên cứu khoa học về sử dụng Smart Contract để thực hiện phân quyền truy cập trong Blockchain.
  + Nghiên cứu tài liệu và video hướng dẫn, để thực hiện đưa Smart Contract, VTK với tính năng phân quyền truy cập vào sử dụng trong mạng Blockchain.
  + Tham khảo cơ sở lý thuyết, thực nghiệm ở trang chủ và các diễn đàn của Quorum Blockchain

**Nội dung 2**: **Tìm hiểu về chuỗi khối ngoài (Sidechain) và cách các node bên trong giao tiếp và chia sẻ dữ liệu giữa hai Blockchain.**

* Mục tiêu:
  + Nắm vững kiến thức cơ bản về Sidechain. Tìm hiểu tổng quan kiến trúc, cách hoạt động của Oracle Nodes và ứng dụng để xây dựng thành sidechain cho hệ thống này.
  + Thiết kế luồng dữ liệu trong quá trình trao đổi. Vai trò và hoạt động của các thành phần gồm node, smart contracts và blockchains.
* Phương pháp:
  + Tham khảo cơ sở lý thuyết [13], thực nghiệm thực tế trước đó [14]
  + Kết nối smart contract của nội bộ blockchain với dữ liệu ngoài chuỗi thông qua trung gian là oracle nodes.

**Nội dung 3**: **Thực nghiệm và đánh giá kết quả.**

* Mục tiêu:
  + Xây dựng hệ thống Sidechain để chia sẻ dữ liệu giữa hai blockchain với VTK kiểm soát quyền truy cập dữ liệu.
  + Đánh giá hiệu năng, độ chính xác và khả năng phát triển của hệ thống.
* Phương pháp:
  + Xây dựng Smart Contract với tính năng phân quyền truy cập và sử dụng VTK để kiểm soát truy cập dữ liệu.
  + Triển khai Etherum Public Blockchain và Quorum Private Blockchain; đưa Smart Contract với các tiêu chí bảo mật và an toàn thông tin lên Blockchain.
  + Xây dựng hệ thống Sidechain để chia sẻ dữ liệu giữa hai Blockchain.
  + Thực hiện các thử nghiệm khác nhau để đánh giá về chi phí, hiệu năng, độ chính xác và độ trễ dự đoán của hệ thống.

## B3. Kết quả nghiên cứu

Sau quá trình nghiên cứu, kết quả dự kiến đạt được như sau:

* Tài liệu báo cáo về mô hình hệ thống giao tiếp liên chuỗi cụ thể là thực trao đổi dữ liệu cho quá trình xác minh dữ liệu giữa hai blockchain khác kiến trúc sử dụng sidechain và kiểm soát truy cập cho dữ liệu trên thông qua khóa có thời hạn và smart contract, đồng thời, cung cấp giao diện tương tác cho người dùng và sử dụng Web App để làm giao diện người dùng.
* Có kết quả thực nghiệm, đưa ra các đánh giá về hiệu năng, chi phí dự tính cho mô hình đã xây dựng.

## B4. Tài liệu tham khảo

[1] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, “Blockchain for healthcare data management: opportunities, challenges, and future recommendations,” Neural Computing and Applications, Jan 2021. [Online]. Available: <https://doi.org/10.1007/s00521-020-05519-w>

[2] M. Rauchs, A. Blandin, K. Bear, and S. B. McKeon, ‘‘2nd global enter-prise blockchain benchmarking study,’’ SSRN Electron. J., Sep. 2019, doi: 10.2139/ssrn.3461765

[3] Y. Pang, ‘‘A new consensus protocol for blockchain interoperability architecture,’’ IEEE Access, vol. 8, pp. 153719–153730, 2020, doi: 10.1109/ACCESS.2020.3017549.

[4] T. Hardjono, A. Lipton, and A. Pentland, ‘‘Toward an interoperability architecture for blockchain autonomous systems,’’ IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1298–1309, Nov. 2020, doi: 10.1109/TEM.2019.2920154.

[5] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, ‘‘Interoperability and synchronization management of blockchain-based decentralized e-Health systems,’’ IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1363–1376, Nov. 2020, doi: 10.1109/TEM.2020.2989779

[6] A. Roehrs, C.A. da Costa, and R. da Rosa Righi. Omniphr: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics, 71:70–81, 2017

[7] Nikki Spence, MBBS Niharika Bhardwaj, and David P Paul III. Ransomware in healthcare facilities: a harbinger of the future? Perspectives in Health Information Management, pages 1–22, 2018.[8] Noor Thamer and Raaid Alubady. A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research. In 2021 1st Babylon International Conference on Information Technology and Science (BICITS), pages 210–216, 2021.

[9] Mu-Hsing Kuo et al. Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3):e1867, 2011.

[10] Y. Zhang, J. Jiang, X. Dong, L. Wang and Y. Xiang, “BeDCV: Blockchain-Enabled Decentralized Consistency Verification for Cross-Chain Calculation,” in IEEE Transactions on Cloud Computing, 2022, doi: 10.1109/TCC.2022.3196937.

[11] M. Sober, G. Scaffino, C. Spanring and S. Schulte, "A Voting-Based Blockchain Interoperability Oracle," 2021 IEEE International Conference on Blockchain (Blockchain), Melbourne, Australia, 2021, pp. 160-169, doi: 10.1109/Blockchain53845.2021.00030.

[12] Sober, M., et al. (2021). A Voting-Based Blockchain Interoperability Oracle. 4th IEEE International Conference on Blockchain (Blockchain), Electr Network.

[13] Sergey Nazarov, Steve Ellis, Dr. Ari Juels (2021). Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks, <https://chain.link/whitepaper>

[14] red·dev. How to Configure and Use Your Own Chainlink Node And External Adapter In Your Avalanche dApp, <https://github.com/red-dev-inc/avalanche-chainlink-tutorial>

[15] 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.

|  |  |
| --- | --- |
| *Ngày 10 tháng 03 năm 2023*  **Chủ nhiệm đề tài**  (Ký và ghi rõ họ tên) | *Ngày 10 tháng 03 năm 2023*  **Giảng viên hướng dẫn**  (Ký và ghi rõ họ tên) |
|  |  |
|  |  |
|  |  |