|  |  |  |
| --- | --- | --- |
| **HỌC VIỆN KỸ THUẬT QUÂN SỰ**  **Khoa công nghệ thông tin**  **---🙚🙘🕮🙚🙘---**    **BÁO CÁO THỰC TẬP CÔNG NGHIỆP**    Đề tài:  XÂY DỰNG HỆ THỐNG QUẢN LÝ Y TẾ ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN      **Sinh viên thực hiện**: Nguyễn Quốc Anh  **Lớp**  : KHMT17  **Lớp** : Công nghệ mạng 15  **Mã sinh viên** : 18150001     |  | | --- | | **Hà Nội, 05/2022** | |  | |

MỤC LỤC

[**LỜI NÓI ĐẦU 1**](#_Toc103782425)

[**I. TÊN ĐỀ TÀI 2**](#_Toc103782426)

[**II. NƠI THỰC TẬP 2**](#_Toc103782427)

[**III. NỘI DUNG THỰC TẬP 2**](#_Toc103782428)

[**1. MỤC ĐÍCH 2**](#_Toc103782429)

[**2. CÁC NỘI DUNG ĐÃ THỰC HIỆN 3**](#_Toc103782430)

[**IV. KẾT QUẢ ĐẠT ĐƯỢC 4**](#_Toc103782431)

[**1. NGHIÊN CỨU LÝ THUYẾT LẬP TRÌNH BLOCKCHAIN TRÊN CÁC TÀI LIỆU CÓ ĐƯỢC 4**](#_Toc103782432)

[**1.1. Tổng quan về Blockchain 4**](#_Toc103782433)

[**1.2. Các khái niệm cơ bản của Blockchain 6**](#_Toc103782434)

[**2. THỰC HÀNH TRÊN DỰ ÁN XÂY DỰNG HỆ THỐNG QUẢN LÝ Y TẾ ỨNG DỤNG CÔNG NGHỆ BLOCKCHAIN 13**](#_Toc103782435)

[**2.1. Tổng quan về dự án 13**](#_Toc103782436)

[**2.2. Xây dựng mạng Blockchain private 14**](#_Toc103782437)

[**2.3. Lập trình Smart Contract 15**](#_Toc103782438)

[**2.4. Lập trình Web3.js 17**](#_Toc103782439)

[**2.5. Lập trình giao diện 18**](#_Toc103782440)

[**3. NHỮNG KỸ NĂNG TÍCH LŨY ĐƯỢC VÀ HƯỚNG PHÁT TRIỂN CỦA BẢN THÂN 18**](#_Toc103782441)

[**3.1. Những kỹ năng tích lũy được 18**](#_Toc103782442)

[**3.2. Hướng phát triển 19**](#_Toc103782443)

[**KẾT LUẬN 20**](#_Toc103782444)

# 

# LỜI NÓI ĐẦU

Blockchain là công nghệ cơ sở dữ liệu sáng tạo, trung tâm của gần như tất cả các loại tiền điện tử. Bằng cách phân phối các bản sao giống hệt nhau của cơ sở dữ liệu trên toàn bộ mạng, blockchain làm cho hệ thống rất khó bị hack hoặc gian lận. Mặc dù tiền điện tử đang được sử dụng phổ biến nhất cho blockchain hiện tại nhưng công nghệ này mang lại tiềm năng phục vụ rất nhiều ứng dụng.

Tính bảo mật và phi tập trung đã khiến blockchain phù hợp để thực hiện các bản ghi dữ liệu sự kiện, hồ sơ y tế, quản lý hộ tịch, quản lý giao dịch, truy xuất nguồn gốc thực phẩm, hay trong các cuộc bầu cử bỏ phiếu… Và trong lĩnh vực y tế, có một vấn nạn từ lâu đã cần phải giải quyết, đó là việc lạm dụng các loại thuốc mà không có sự kê đơn hay chỉ định của bác sĩ hay những người có thẩm quyền, với một vài trường hợp, nó có thể gây ra những tình trạng bệnh lí nặng hơn hay phụ thuộc vào thuốc như việc lạm dụng các loại thuốc giảm đau. Đôi khi nó còn ảnh hưởng tới cả nhân loại như việc lạm dụng thuốc kháng sinh đã tạo ra những vi khuẩn kháng kháng sinh… Để đảm bảo sự minh bạch và rõ ràng trong việc quản lí đơn thuốc nói riêng hay quản lí hồ sơ y tế nói chung, việc ứng dụng công nghệ Blockchain là vô cùng cấp thiết.

Vì vậy, em lựa chọn đề tài “Sử dụng công nghệ Blockchain để ứng dụng trong bài toán kiểm tra tính toàn vẹn của dữ liệu trong hệ thống quản lý y tế”.

# I. KẾT QUẢ ĐẠT ĐƯỢC

## 1. TỔNG QUAN VỀ LÝ THUYẾT

### 1.1. Tổng quan về Blockchain

#### 1.1.1. Cơ chế hoạt động của Blockchain

Cái tên blockchain không phải ngẫu nhiên được chọn để sử dụng như bây giờ. Blockchain thường được mô tả là một “chuỗi” được tạo thành từ các “khối” dữ liệu riêng lẻ. Khi dữ liệu mới được thêm vào mạng định kỳ, một “khối” mới sẽ được tạo và gắn vào “chuỗi”. Điều này liên quan đến việc tất cả các nút cập nhật phiên bản blockchain của họ để tất cả đều giống hệt nhau.

Cách các khối mới này được tạo ra là chìa khóa giải thích tại sao blockchain được coi là an toàn cao. Phần lớn các nút phải xác minh và xác nhận tính hợp pháp của dữ liệu mới trước khi một khối mới có thể được thêm vào sổ cái kỹ thuật số. Đối với tiền điện tử, chúng có thể liên quan đến việc đảm bảo rằng các giao dịch mới trong một khối không phải là gian lận hoặc tiền chưa được sử dụng nhiều hơn một lần. Điều này khác với cơ sở dữ liệu hoặc bảng tính độc lập, nơi một người có thể thực hiện các thay đổi mà không cần giám sát.

Sau khi có sự đồng thuận, khối sẽ được thêm vào chuỗi và các giao dịch cơ bản được ghi lại trong sổ cái phân tán. Các khối được liên kết với nhau một cách an toàn, tạo thành một chuỗi kỹ thuật số an toàn từ đầu cho tới cuối sổ cái. Các giao dịch thường được bảo mật bằng mật mã, có nghĩa là các nút cần giải các phương trình toán học phức tạp để xử lý một giao dịch.

#### 1.1.2. Phân loại

Có cả blockchain công khai và riêng tư. Trong một blockchain công khai, bất kỳ ai cũng có thể tham gia, nghĩa là họ có thể đọc, viết hoặc kiểm tra dữ liệu trên blockchain. Rất khó để thay đổi các giao dịch được đăng nhập trong một blockchain công khai vì không có cơ quan quyền lực duy nhất nào kiểm soát các nút của blockchain.

Trong khi đó, một blockchain riêng tư được kiểm soát bởi một tổ chức hoặc nhóm. Chỉ có tổ chức hoặc nhóm đó mới có thể quyết định ai được mời vào hệ thống, sau đó nó có quyền quay lại và thay đổi chuỗi khối. Quy trình blockchain riêng tư này tương tự như một hệ thống lưu trữ dữ liệu nội bộ ngoại trừ việc trải rộng trên nhiều nút để tăng tính bảo mật.

Trong đề tài lần này, em sẽ xây dựng ứng dụng trên một mạng Blockchain riêng tư, sử dụng công cụ Ganache.

### Các khái niệm và công nghệ sử dụng

##### Giới thiệu về các cơ chế đồng thuận

Cơ chế đồng thuận được biết đến chính là một trong đặc tính quan trọng ảnh hưởng khả năng mở rộng và tính an toàn của mỗi nền tảng tiền mã hóa. Cơ chế này tồn tại nhằm ngăn chặn vấn đề chi tiêu 2 lần trên Blockchain (double spending). Xét từ góc độ đầu tư, cơ chế đồng thuận là một trong những tiêu chí quan trọng khi lựa chọn bất kỳ đồng tiền mã hóa nào.

Cơ chế đồng thuận trong tiếng Anh là Consensus Mechanism.

Cơ chế đồng thuận là một cơ chế chịu lỗi được sử dụng trong các hệ thống máy tính và chuỗi khối để đạt được thỏa thuận mong muốn về một giá trị dữ liệu hoặc một trạng thái duy nhất của mạng giữa các qui trình phân bổ hoặc hệ thống đa tác nhân. Nó rất hữu ích trong việc lưu trữ hồ sơ so với các cơ chế khác.

Có nhiều loại thuật toán về cơ chế đồng thuận khác nhau hoạt động trên các nguyên tắc khác nhau:

##### Proof-of-work (PoW) – Minh chứng làm việc:

Khởi tổ của giao thức đồng thuận và đứa con tinh thần của Satoshi Nakamoto, giao thức chứng minh công việc (PoW) liên quan đến những người thợ mỏ giải các câu đố mã hóa phức tạp, mà qua đó họ nhận được phần thưởng dưới dạng đồng coin hoặc đồng token.

Ưu điểm: Là giao thức đầu tiên, Proof-of-work (PoW) đã chứng minh khả năng phục hồi của nó trước các cuộc tấn công nội bộ và bên ngoài.

Nhược điểm: Proof-of-work (PoW) bị chỉ trích vì nhiều lý do. Proof-of-work (PoW) tiêu thụ nhiều năng lượng, với một số ước tính chỉ ra năng lượng mạng Bitcoin tiêu thụ ở cùng cấp độ với 159 quốc gia. Các nhà phê bình của Bitcoin như Andrew Tayo đã chỉ ra rằng phần lớn năng lượng này bị lãng phí, vì chỉ có một thợ mỏ cuối cùng có thể khai thác từng khối (được chấp nhận), bất kể có bao nhiêu người tham gia cuộc đua đến đó trước.

##### Proof-of-stake (PoS) – Minh chứng cổ phần:

Proof-of-stake (PoS) lần đầu tiên được hình thành như một cách để tránh những vấn đề cố hữu với Proof-of-work (PoW), chẳng hạn như tiêu thụ năng lượng. Trong mô hình PoS, những người nắm giữ những đồng coin có thể đặt cược chúng vào khả năng khối tiếp theo là chính xác. Nếu có, họ nhận được phần thưởng. Nếu ai đó đặt cược những đồng coin vào một khối mà khối đó có chứa các giao dịch gian lận, họ sẽ bị ‘phạt’ giá trị cổ phần (phần cược) của họ.

Ưu điểm: Proof-of-stake (PoS) tiêu thụ ít năng lượng hơn Proof-of-work (PoW). Proof-of-stake (PoS) cũng tích cực trừng phạt gian lận, ngăn chặn hành vi lừa đảo giữa các người xác nhận.

Nhược điểm: Khi các nút xác nhận không đóng góp sức mạnh tính toán – được gọi là vấn đề “không có cổ phần” – có nguy cơ tăng lên đó là PoS Blockchains có thể thấy nhiều nhánh hơn PoW. Ngoài ra, Proof-of-stake (PoS) ủng hộ những người có nhiều đồng coin nhất, đồng thời thúc đẩy tập quyền vì những người nắm giữ giàu có hơn có thể đặt cược nhiều hơn. Đối với PoS coin NXT, nó đã được chứng minh được rằng làm thế nào một người nắm cổ phần có thể tăng vững chắc số cổ phần của họ đến mức họ sẽ sở hữu hơn 90% số đồng coin.

##### Delegated PoS (dPoS) – PoS được ủy quyền:

PoS được ủy quyền được phát minh bởi Daniel Larimer, đồng sáng lập của Steem và CTO của EOS, cả hai đều sử dụng dPoS. Ở đây, mạng lưới sẽ bầu cho ‘Nhân Chứng’, người đạt được sự đồng thuận để thêm khối tiếp theo. Tương tự như mô hình PoS chuẩn, trọng số biểu quyết của người tham gia mạng được xác định bằng số lượng token (mã thông báo) mạng mà họ nắm giữ.

Ưu điểm: PoS được ủy quyền làm giảm thời gian tạo khối, vì càng ít bên tham gia vào một sự đồng thuận từ đó tăng tốc độ ra quyết định. Bằng cách tránh sử dụng ASIC, nó khuyến khích phân cấp – nhưng với một số cảnh báo, như được nêu ra dưới đây.

Khuyết điểm: Việc sử dụng ‘Nhân Chứng’ có nghĩa là sự phân cấp hoàn toàn không bao giờ đạt được. Xem xét sự khác biệt giữa một nền dân chủ đầy đủ – tất cả các công dân bỏ phiếu cho tất cả các vấn đề – và một nền dân chủ đại diện, nơi các đại biểu được bầu để đại diện cho cử tri.

##### IBFT (Istanbul Byzantine Fault Tolerant)

IBFT (Istanbul Byzantine Fault Tolerant) là một cơ chế đồng thuận thay thế cho Proof of Work trong mạng Ethereum.

IBFT mang nhiều hiệu quả và lợi thế hơn khi xây dựng những mạng blockchain riêng tư thay vì công khai. Thuật toán PoW nổi tiếng là tốn kém cả về phần cứng và điện năng. Chi phí này là có chủ đích, để ngăn bất kỳ ai dễ dàng chiếm đoạt mạng và do đó PoW rất phù hợp cho các tình huống có toàn quyền phân quyền, nơi bất kỳ ai (kể cả những kẻ tấn công) đều có thể tham gia. Tuy nhiên, các nút trong mạng liên hợp / mạng riêng tư được sử dụng bởi các doanh nghiệp về bản chất được tin cậy hơn so với các mã trong chuỗi công khai. Do đó, cơ chế đồng thuận PoW có thể quá nặng nề và các cơ chế khác có thể cung cấp sự tin tưởng “đủ” để chạy cho một hệ thống phân tán. Tương tự như vậy, Proof of Stake có thể ít được sử dụng trong môi trường các doanh nghiệp, bởi vì việc thanh toán cho phí gas ít quan trọng hơn trong một mạng lưới được bảo mật cao. Vì các nút mạng không cần thu phí trong mạng, PoS sẽ đưa ra các yêu cầu không liên quan.

Xem xét những đánh đổi này, Proof of Authority (PoA) nổi lên như một giải pháp tốt nhất có thể, sử dụng một hệ thống theo đó các nút trong mạng được cấp đặc quyền tạo ra các khối mới cho chuỗi bằng cách sử dụng hệ thống vòng lặp hoặc tùy ý khác.

IBFT là một trong nhiều biến thể của PoA và cung cấp các lợi ích sau:

Immediate block finality: Chỉ có 1 khối được đề xuất ở độ cao chuỗi nhất định. Do đó, chuỗi đơn sẽ loại bỏ các khối phân nhánh, không chú ý và rủi ro rằng một giao dịch có thể được “hoàn tác” một lần trên chuỗi sau đó.

Reduced time between blocks: Nỗ lực cần thiết để xây dựng và xác thực các khối được giảm đáng kể (đặc biệt đối với PoW), làm tăng đáng kể thông lượng của chuỗi.

High data integrity and fault tolerance: IBFT sử dụng một nhóm validator để đảm bảo tính toàn vẹn của mỗi khối được đề xuất. Phần lớn (~ 66%) trong số các validator này được yêu cầu ký vào khối trước khi chèn vào chuỗi, khiến cho việc giả mạo khối trở nên rất khó khăn. Quyền "lãnh đạo" của nhóm cũng thay đổi theo thời gian - đảm bảo một nút bị lỗi không thể gây ảnh hưởng lâu dài đến chuỗi.

Operationally flexible: Nhóm validator có thể được sửa đổi kịp thời, đảm bảo nhóm chỉ chứa các nút được tin cậy đầy đủ.

#### 1.2.1. Giới thiệu về Ethereum

Ethereum là nền tảng điện toán phân tán, mã nguồn mở dựa trên công nghệ chuỗi khối (Blockchain) có khả năng thực thi hợp đồng thông minh (Smart Contract) - tức là điều khoản được ghi trong hợp đồng sẽ được thực thi một cách tự động khi các điều kiện trước đó được thỏa mãn, không ai có thể can thiệp vào. Đồng thời, Ethereum cũng cho phép các nhà phát triển xây dựng các ứng dụng phi tập trung (DApps) và các tổ chức tự trị phi tập trung (DAOs). Trong đó:

Các ứng dụng phi tập trung (DApps - Decentralized Application) là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà được lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào.

Các tổ chức tự trị phi tập trung (DAOs - Decentralized Autonomous Organizations) là một tổ chức được vận hành bởi các thành viên dựa trên một bộ quy tắc được mã hóa bằng code. Tất cả các thành viên đều có quyền biểu quyết các quyết định quan trọng của DAOs. Đổi lại, các thành viên tham gia DAOs phải có phần thưởng khi tham gia vận hành DAOs.

EVM nói một cách đơn giản là một phần trong mạng Ethereum có nhiệm vụ xử lý việc triển khai và thực thi trên smart contract. EVM có trên tất cả các client (node) của mạng Ethereum, hướng đến mục tiêu như là một máy tính phi tập trung toàn cầu.

#### 1.2.2. Giới thiệu về Smart Contract

* Smart Contract (Hợp Đồng Thông Minh) là một thuật ngữ mô tả một bộ giao thức đặc biệt có khả năng tự động thực hiện các điều khoản, các thoả thuận giữa các bên trong hợp đồng (ở trường hợp này là các hệ thống máy tính) nhờ sự hỗ trợ của công nghệ Blockchain. Toàn bộ hoạt động của Smart Contract được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài, hay thông qua một bên thứ ba trung gian.
* Những giao dịch được thực hiện bằng các hợp đồng thông minh rất minh bạch, có thể dễ dàng truy xuất được và không thể bị can thiệp hoặc đảo chiều. Các điều khoản trong Smart Contract tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình (Với mạng Ethereum, ngôn ngữ lập trình sử dụng Solidity).
* Smart contract đã sử dụng được tất cả những điểm mạnh của công nghệ Blockchain
* Tính bảo mật Smart contract được mã hóa và phần phối về cho các node. Các thứ này bảo đảm nó sẽ không bị thất lạc hay sửa đổi mà không được bạn cho phép.
* Hiệu quả về kinh tế và nhanh gọn Hầu hết các công đoạn đều được tư động hóa, và gần như loại bỏ bên trung gian.
* Tiêu chuẩn hóa
* Tuy nhiên vẫn có những nhược điểm :
* Nhân tố con người: Vì toàn bộ phần mã được soạn thảo bởi con người và họ vẫn có thể mắc lỗi. Nếu smart contract đã được tải lên Blockchain, các nhà lập trình sẽ không thể nào thay đổi được nó. Một ví dụ nổi tiếng về nhận tố con người đó chính là sự kiện DAO. Lỗi lập trình đã bị một số tin tặc phát hiện và tận dụng, từ đó cướp đoạt đến 60 triệu tiền vốn của người dung.
* Tình trạng pháp lý chưa rõ ràng: Hiện tại, Smart Contract vẫn chưa được quản lí bởi bất kì chính phủ nào cả. Vì thế cho nên vẫn tiềm ẩn khả năng xuất hiện mâu thuẫn nếu như các thể chế quả lí quyết định xây dựng bộ khung pháp lý dành cho hình thức smart contract còn khá mới mẻ này.
* Chi phí thực hiện: Smart Contract không thể nào được lập nên mà không cần thông qua công đoạn lập trình. Do đó, điều cần thiết là phải có một chuyên gia lập trình dày dạn kinh nghiệm trong đội ngũ phát triển để hạn chế tối đa những sai sót có thể xảy ra đối với hợp đồng và bảo đảm cơ sở hạ tầng của công ty tương thích được với công nghệ Blockchain.

#### Giới thiệu về Solidity

* Solidity là một ngôn ngữ high-level dùng cho ứng dụng vào Smart Contract. Nó là một ngôn ngữ hướng đối tượng được thiết kế dành riêng cho Ethereum Virtual Machine.
* Solidity là ngôn ngữ lập trình được xây dựng dưới sự thừa kế những đặc điểm phù hợp của các ngôn ngữ lập trình khác, đặc biệt là những đặc tính liên quan đến contract. Cũng tương tự như các ngôn ngữ lập trình khác, Solidity sử dụng những kiểu dữ liệu thông dụng như: kiểu số nguyên - Integer, kiểu dữ liệu 0,1 hay tương ứng với true, false - boolean, kiểu chuỗi ký tự - string literals,... Ngoài ra còn rất nhiều những kiểu dữ liệu tương thích với Solidity như kiểu mảng, toán tử, enum,... Nhìn chung, ngôn ngữ Solidity cho phép người dùng sử dụng gần như tất cả các kiểu dữ liệu phổ biến hiện nay.

=> Như vậy, với mạng Ethereum, ngôn ngữ sử dụng cho lập trình Smart Contract sẽ là Solidity.

#### Giới thiệu về các chuẩn ERC

**ERC** viết tắt của từ **Ethereum Request for Comment**, là một tiêu chuẩn của các Token phát triển trên nền tảng Blockchain của **Ethereum**. ERC giúp xác định hình thức của việc tạo và cấu trúc nên một Token thông qua việc lập trình **Smart Contract** (hợp đồng thông minh). Hiện tại có khá nhiều các chuẩn ERC như ERC20, ERC777, ERC721, ERC948,..Cách viết của các token này có thể là ERC20, ERC 20 hoặc ERC-20.

Trong đề tài lần này, với mục đích và ứng dụng đã được đề ra, chúng ta sẽ sử dụng chuẩn ERC-721. ERC-721 được khởi nguồn từ một dự thảo EIP (đề xuất cải tiến Ethereum) của Dieter Shirley – CTO của Dapper Labs, sau đó đã trở thành cơ sở cho trò chơi CryptoKitties. ERC-721 mang tới một tiêu chuẩn cho NFT. Nói cách khác, loại token này là duy nhất và có giá trị khác với các token khác từ cùng một hợp đồng thông minh (có thể khác ở tuổi thọ, mức độ hiếm, hình ảnh trực quan hoặc bất kì điểm khác biệt nào).

Tất cả các NFT đều có một biến số uint256 riêng được gọi là TokenID. Vì vậy, đối với bất kỳ hợp đồng ERC-721 nào, địa chỉ hợp đồng cặp (hay uint256 TokenID) phải là duy nhất trên toàn bộ mạng lưới. Điều đó có nghĩa rằng, một Dapp có thể có một “bộ chuyển đổi” sử dụng TokenID làm dữ liệu đầu vào và xuất ra một hình ảnh của một cái gì đó hay ho như các nhân vật zombie, vũ khí, kỹ năng hoặc những nhân vật amazing kitty.

ERC-721 cung cấp các chức năng như chuyển token từ tài khoản này sang tài khoản khác, tra được số dư token hiện tại của tài khoản, tra được thông tin chủ sở hữu của một token cụ thể và cung cấp thông tin tổng nguồn cung token đang có sẵn trên mạng lưới. Bên cạnh đó, nó còn có một số chức năng khác như phê duyệt cho một lượng token từ một tài khoản có thể được di chuyển bởi một tài khoản khác của bên thứ ba.

##### 1.2.5. Giới thiệu về framework web3

* Web3.js là một thư viện JavaScript mã nguồn mở (GNU Lesser General Public License phiên bản 3) được xây dựng bởi Ethereum Foundation, bao gồm các chức năng giao tiếp với các nút Ethereum thông qua giao thức JavaScript Object Notation – Remote Procedure Call (JSON-RPC) . Nói cách khác, nó là một thư viện JavaScript hỗ trợ các nhà phát triển tương tác với chuỗi khối Ethereum.
* Web3.js có một lớp chính được gọi là web3. Hầu hết các chức năng của thư viện có thể được tìm thấy trong danh mục này. 5 mô-đun khác tạo nên web3js là:
  + web3-eth
  + web3-shh
  + web3-bzz
  + web3-net
  + web3-utils
    - 1. **Web3-eth**
* Mô-đun web3-eth chứa các chức năng cho phép người dùng web3.js tương tác với chuỗi khối Ethereum. Cụ thể, các chức năng này có thể tương tác với các hợp đồng thông minh, tài khoản thuộc sở hữu bên ngoài, các nút, khối được khai thác và các giao dịch. Dưới đây là ba ví dụ minh họa:
* Chức năng của \_web3.eth.getBalance\_ là lấy số dư Ethereum của một địa chỉ trong một khối cụ thể
* Vai trò của \_web3.eth.signTransaction\_ là ký giao dịch
* Chức năng của \_web3.eth.sendSignedTransaction\_ là gửi giao dịch đã ký đến chuỗi khối Ethereum.
  + - 1. **Web3-shh**
* Chức năng của mô-đun web3-shh là cho phép bạn tương tác với giao thức Whisper. Whisper là một giao thức truyền thông điệp, mục đích của nó là truyền thông điệp dễ dàng và truyền thông không đồng bộ mức thấp. Dưới đây là hai ví dụ minh họa:
* \_web3.shh.post\_post gửi tin nhắn Whisper cho web
* \_web3.shh.subscribe\_Tạo đăng ký tin nhắn Whisper đến
  + - 1. **Web3-bzz**
* Chức năng của mô-đun web3-bzz là cho phép bạn tương tác với Swarm. Nó là một nền tảng lưu trữ phi tập trung và dịch vụ phân phối nội dung có thể được sử dụng để lưu trữ các tệp như hình ảnh hoặc video cho các ứng dụng phi tập trung. Dưới đây là hai ví dụ minh họa:
* Chức năng của \_web3.bzz.upload\_ là cho phép bạn tải các tệp và thư mục lên Swarm
* Vai trò của \_Web3.bzz.download\_ là cho phép bạn tải xuống các tệp và thư mục từ Swarm
  + - 1. **Web3-net**
* Chức năng của mô-đun web3-net là cho phép bạn tương tác với các thuộc tính mạng của các nút Ethereum. Thông qua web3-net, bạn có thể sử dụng giao thức được liên kết với thông tin bạn cần lấy, sau đó là .net (được chỉ định bằng \* ở đây, có nghĩa là chọn web.eth.net, web3.shh.net hoặc web3.bzz.net) để tìm kiếm Thông tin về nút này. Dưới đây là hai ví dụ minh họa:
* web3. \*. net.getID trả về ID mạng
* web3. \*. net.getPeerCount trả về số lượng đồng nghiệp được kết nối với nút
  + - 1. **Web3-utils**
* Mô-đun web3-utils cung cấp cho bạn các chức năng tiện ích, có thể được sử dụng trong các ứng dụng phi tập trung Ethereum và các mô-đun web3.js khác. Các chức năng tiện ích có thể được sử dụng lại, giúp việc viết mã dễ dàng hơn và rất phổ biến trong JavaScript và các ngôn ngữ lập trình khác. Web3-utils chứa các hàm tiện ích để chuyển đổi số, xác minh xem các giá trị có đáp ứng các điều kiện nhất định hay không và tìm kiếm tập dữ liệu. Dưới đây là ba ví dụ minh họa:
* \_web3.utils.toWei\_ chuyển đổi ether sang Wei
* \_web3.utils.hexToNumberString\_ chuyển đổi một giá trị thập lục phân thành một chuỗi
* web3.utils.isAddress, để xác minh xem một chuỗi cụ thể có phải là địa chỉ Ethereum hợp lệ hay không.

## 2. THỰC HÀNH

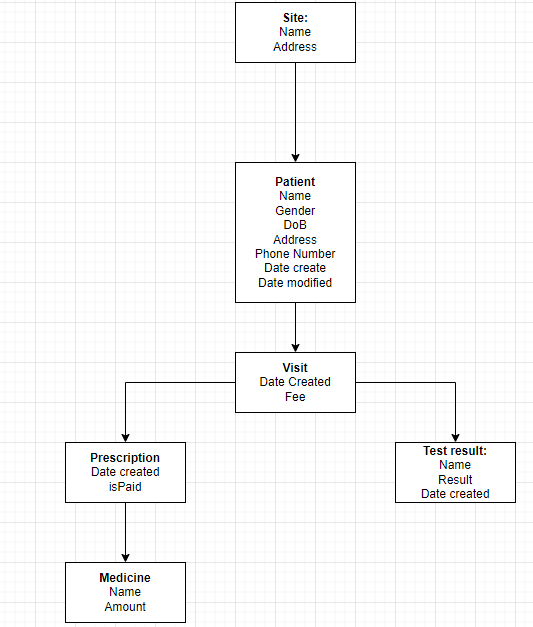
### 2.1. Tổng quan về ứng dụng

Mục đích: Ứng dụng được xây dựng trên nền tảng phi tập trung với mục đích lưu trữ dữ liệu và đảm bảo tính toàn vẹn, minh bạch của dữ liệu, cụ thể là dữ liệu y tế. Những dữ liệu được lưu sẽ là thông tin của những người bệnh nhân trong và sau quá trình chữa trị tại các bệnh viện. Để thực hiện được yêu cầu này, việc ứng dụng công nghệ Blockchain là giải pháp phù hợp, nơi mà dữ liệu sẽ không thể bị chỉnh sửa hay xóa đi, tất cả những thành viên tham gia mạng đều có thể thấy được những dữ liệu trên Blockchain đó.

Các phần chính của ứng dụng:

* Mạng Blockchain riêng tư để đảm bảo tính bảo mật của dữ liệu. Ganache để dựng một mạng Blockchain private để lưu trữ dữ liệu
* Xây dựng các Smart Contracts theo cấu trúc dữ liệu được đặt ra để tổ chức hệ thống dữ liệu trong khuôn khổ hệ thống quản lí y tế
* Xây dựng giao diện hỗ trợ tương tác giữa người dùng và mạng Blockchain

### 2.2. Cấu trúc dữ liệu



- Site: lưu trữ dữ liệu của một bệnh viện (hoặc 1 chi nhánh của bệnh viện). Lưu trữ thông tin các bệnh nhân đã thăm khám tại đây

- Patient: lưu trữ dữ liệu của một bệnh nhân của một Site. Lưu trữ các thông tin cá nhân và thông tin của các lần thăm khám của bệnh nhân đó.

- Visit: lưu trữ thông tin của lần thăm khám của bệnh nhân. Lưu trữ thông tin bao gồm đơn thuốc và các kết quả xét nghiệm trong quá trình thăm khám của bệnh nhân.

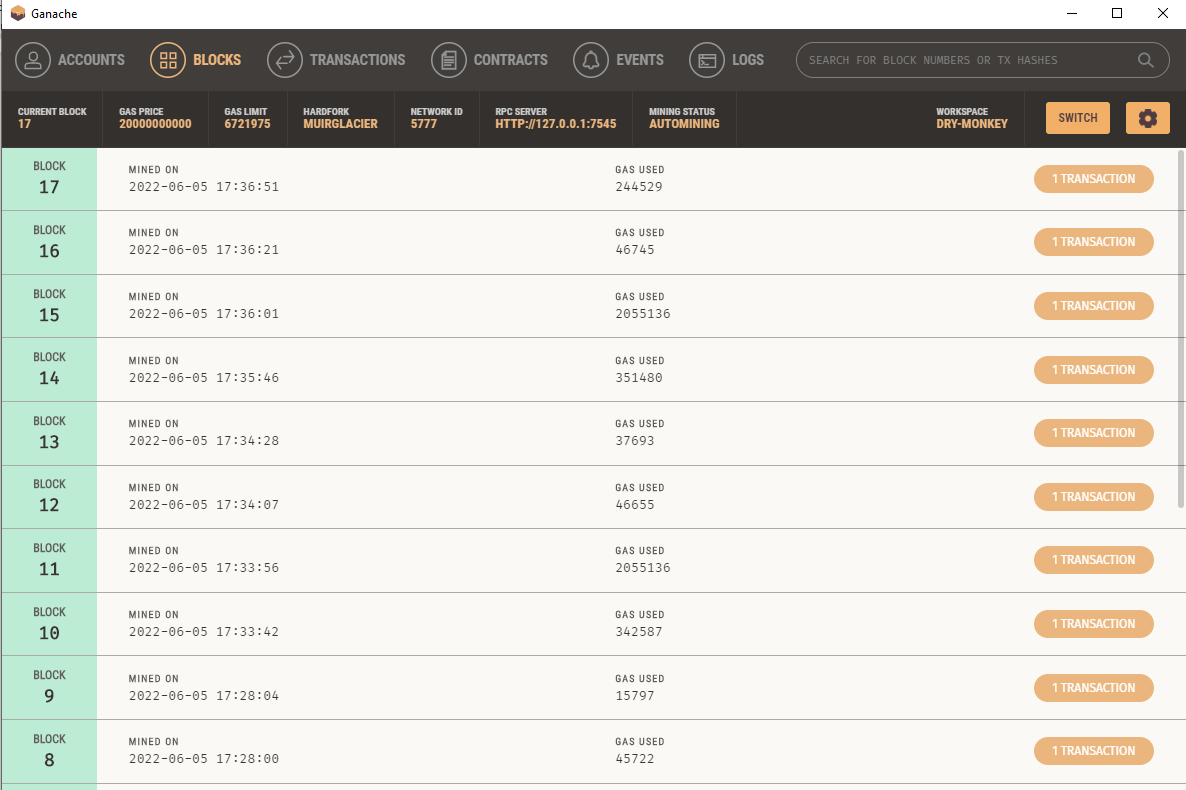
- Test Result: lưu trữ thông tin của một xét nghiệm và kết quả của nó.

- Prescription: lưu trữ thông tin của một đơn thuốc, bao gồm tình trạng trả phí và các loại thuốc đi kèm.

- Medicine: lưu trữ thông tin của loại thuốc và số lượng, liều dùng

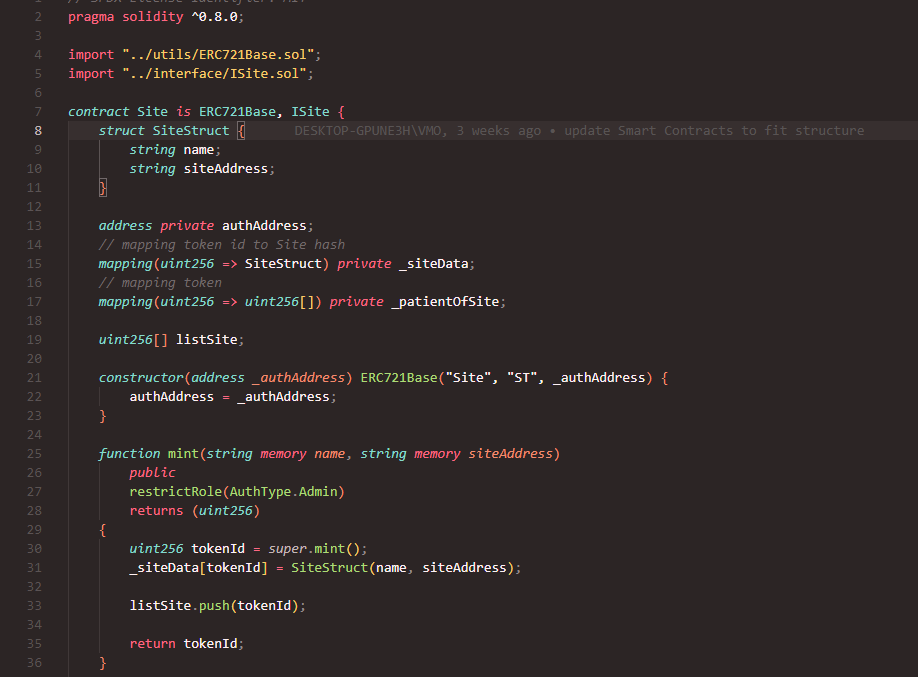
### 2.3. Xây dựng mạng Blockchain

- Trong môn học này, em sẽ sử dụng Ganache để dựng một mạng Blockchain private để lưu trữ các Smart Contracts cũng như theo các thông tin theo cấu trúc dữ liệu

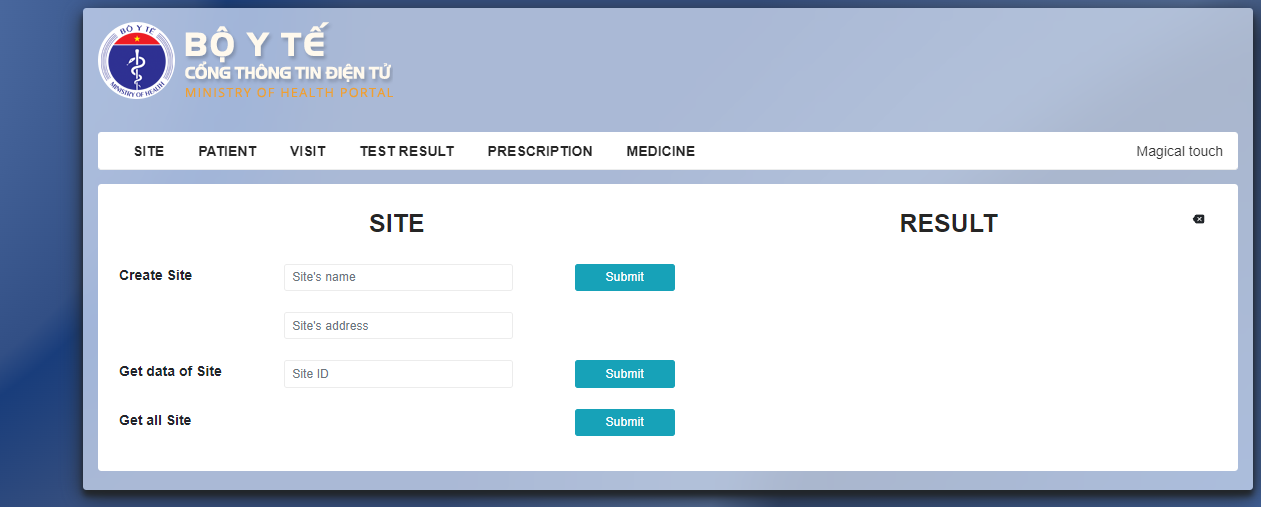


### 2.4. Lập trình Smart Contract

- Sử dụng ngôn ngữ Solidity cho phần code và IDE Remix Ethereum cho phần deploy:



### 2.4. Lập trình giao diện



### 2.5. Lập trình Web3js

- Sử dụng web3js để tương tác giữa front-end và blockchain



## 3. HƯỚNG PHÁT TRIỂN

### 3.1. Đánh giá

Trong giới hạn môn học, ứng dụng quản lí y tế trên đã được xây dựng dựa trên những framework cơ bản của Blockchain, từ việc xây dựng những Smart Contract đến deploy trên mạng Blockchain private.

Việc xây dựng đề tài đã ứng dụng được Blockchain vào 1 cách thiết thực, thay vì nó đang được sử dụng trong việc tạo ra những game finance thường bị mang ý nghĩa “lùa gà” trong thời điểm hiện tại.

### 3.2. Hướng phát triển

Trải qua quá trình học hỏi và nghiên cứu tài liệu cũng như xây dựng đề tài, còn có rất nhiều tính năng, chức năng cần được xây dựng, nâng cấp:

* Xây dựng mạng Blockchain private trên nền tảng có ý nghĩa hơn khi áp dụng vào thực tế các doanh nghiệp (VD: Hyperledger Fabric…)
* Bảo mật thông tin của người dùng. Hiện tại dữ liệu khi đẩy lên Blockchain đang public những thông tin cá nhân, điều vô cùng nhạy cảm khi những dữ liệu trên Blockchain là không thể bị xóa hay sửa đổi, vì vậy cần phát triển tính năng bảo mật mã hóa 2 chiều cho những dữ liệu của người dùng, tang độ tin cậy cho ứng dụng.
* Phát triển giao diện bắt mắt, thân thiện hơn với người dùng.

# KẾT LUẬN

Qua việc tìm hiểu và nghiên cứu trong suốt quá trình thực tập công nghệ thông tin. Em đã nắm bắt được nhiều kiến thức bổ ích hỗ trợ cho công việc và định hướng tương lai, đồng thời rút ra được nhiều kinh nghiệm thực tế.

Qua đó, em thấy được tầm quan trọng của công nghệ Blockchain trong thời đại ngày nay, khi nhu cầu bảo mật và quyền riêng tư thông tin của người dùng ngày càng một nâng cao, thì việc nâng cấp công nghệ để chạy theo nhu cầu đó cũng là một cơ hội cho những sinh viên còn trẻ và đầy nhiệt huyết như em. Em xin cám ơn!