**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**



VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

-------------------------------------------



**BÁO CÁO PROJECT III**

**Đề tài: NGHIÊN CỨU SMART CONTRACT**

**TRÊN NỀN TẢNG BLOCKCHAIN**

**Giảng viên: Nguyễn Duy Hiệp**

Sinh viên thực hiện: Kiều Minh Hướng

Mã số sinh viên: 20183928

Lớp: Công nghệ thông tin 03 – K63

Mã học phần: IT3940

Hà Nội, 9-2021

# **LỜI CẢM ƠN**

Công nghệ đang phát triển từng ngày và đối với sinh viên học ngành công nghệ thông tin như em, việc tìm hiểu những công nghệ mới là vô cùng cần thiết để có thể tự tạo cho mình hành trang tốt nhất bước vào môi trường làm việc sau này. Đối với môn Project III, sau khi được thầy Nguyễn Duy Hiệp hướng dẫn, em đã quyết định lựa chọn đề tài phù hợp với định hướng của mình. Trong quá trình làm project này, em rất vui vì luôn có thể nhận được sự trợ giúp của thầy. Từ tận đáy lòng mình, em vô cùng biết ơn vì điều đó.

Em cũng đã cố gắng để hoàn thiện sản phẩm của mình. Tuy nhiên, do kiến thức cũng như kinh nghiệm thực tế, tư duy còn nhiều hạn chế, giới hạn trong phạm vi hiểu biết của sinh viên nên sản phẩm mới chỉ dừng lại ở mức khá đơn giản và không tránh khỏi những thiếu sót. Em rất mong nhận được sự quan tâm và đóng góp ý kiến của thầy để project này được hoàn thiện hơn.

Em xin chân thành cám ơn thầy!

# **MỤC LỤC**

[**LỜI CẢM ƠN** 1](#_Toc83695040)

[**MỤC LỤC** 2](#_Toc83695041)

[**LỜI MỞ ĐẦU** 3](#_Toc83695042)

[**CHƯƠNG I: TỔNG QUAN VỀ HỢP ĐỒNG THÔNG MINH** 6](#_Toc83695049)

[**1.1. Khái niệm blockchain** 6](#_Toc83695050)

[**1.2. Khái niệm hợp đồng thông minh** 6](#_Toc83695051)

[**1.3. Ứng dụng của hợp đồng thông minh** 7](#_Toc83695052)

[**\*/ Tiểu kết chương 1:** 9](#_Toc83695053)

[**CHƯƠNG II: PHÂN TÍCH PROJECT SMART CONTRACT** 10](#_Toc83695054)

[**2.1. Hệ thống Blockchain** 10](#_Toc83695055)

[**2.2. Xây dựng API** 13](#_Toc83695056)

[**\*/ Tiểu kết chương 2:** 22](#_Toc83695057)

[**CHƯƠNG III: ĐÁNH GIÁ PROJECT** 23](#_Toc83695058)

[**3.1. Ưu điểm** 23](#_Toc83695059)

[**3.2. Nhược điểm** 23](#_Toc83695060)

[**3.3. Định hướng phát triển** 23](#_Toc83695061)

[**\*/ Tiểu kết chương 3:** 25](#_Toc83695062)

[**KẾT LUẬN** 26](#_Toc83695063)

[**TÀI LIỆU THAM KHẢO** 27](#_Toc83695064)

[**PHỤ LỤC** 28](#_Toc83695065)

# **LỜI MỞ ĐẦU**

## **1. Lý do chọn đề tài**

Chúng ta đang sống trong thời kỳ của kỷ nguyên kỹ thuật số gắn liền với những đột phá về công nghệ, trong đó công nghệ thông tin (CNTT) đóng vai trò là công nghệ cốt lõi. CNTT không chỉ là một ngành kinh tế mà còn là động lực quan trọng để giúp các ngành khác phát triển. Trong tương lai, cách sống, làm việc, sản xuất của con người sẽ được thay đổi mạnh mẽ. Công nghệ mới sẽ sắp xếp lại thị trường lao động, nhiều việc làm truyền thống sẽ mất đi, nhiều công việc mới, cơ hội mới sẽ xuất hiện thay thế.

Mặc dù được phát triển từ lâu nhưng nhiều người biết đến Blockchain hơn khi nó gắn liền với Bitcoin. Blockchain là một "siêu công nghệ" với vô vàn công dụng nổi bật và được ứng dụng trong rất nhiều lĩnh vực trong cuộc sống.

Blockchain hiện đang là xu thế công nghệ của thời đại, đang được áp dụng rất nhiều ngành nghề và lĩnh vực khác nhau. Có những quốc gia hay doanh nghiệp lớn bỏ rất nhiều tiền và thời gian để đầu tư và nghiên cứu công nghệ blockchain bởi tính ứng dụng tĩnh tiễn cao và độ bảo mật tuyệt vời của nó.

Đối với em, một sinh viên có định hướng theo ngành An toàn thông tin, mật mã, công nghệ chuỗi khối là một khía cạnh rất quan trọng và phải có kiến thức vững vàng. Vì vậy, sau khi nhận được sự hướng dẫn của thầy Nguyễn Duy Hiệp, em đã quyết định lựa chọn đề tài: “**Nghiên cứu Smart Contract trên nền tảng Blockchain**”. Do kiến thức của em còn hạn chế, trong project cũng như báo cáo này vẫn còn nhiều thiếu sót, hi vọng sẽ nhận được sự góp ý của thầy để kết quả đạt được qua Project này của em là tốt nhất có thể.

## **2. Tổng quan về đề tài**

Blockchain là một công nghệ trong đó toàn bộ dữ liệu được mã hóa thành các khối và nối với nhau tạo thành chuỗi dài. Mỗi khi có một thông tin hay một giao dịch mới phát sinh, thông tin cũ sẽ không bị mất đi mà thay vào đó là thông tin mới sẽ được lưu vào một khối (block) mới và gắn nối tiếp vào khối cũ tạo thành một chuỗi (chain).

Hơn thế nữa, thông tin của blockchain không chỉ nằm trên một máy chủ duy nhất mà nó sẽ được tự động phân tán và sao lưu trên nhiều máy chủ khác nhau có kết nối với hệ thống blockchain, từ đó tất cả mọi người đều có thể nhìn thấy và kiểm tra được giao dịch của mình. Điều này ngăn cản việc chỉnh sửa hay gian lận, thông tin được đảm bảo an toàn và minh bạch. Nổi bật của ứng dụng blockchain chính là bitcoin, một đồng tiền điện tử nổi tiếng nhất thế giới và đã được nhiều quốc gia công nhận là một loại tiền tệ.

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. Tại Việt Nam, công nghệ Blockchain được ứng dụng chủ yếu trong các lĩnh vực: dịch vụ tài chính (hơn 83%), chuỗi cung ứng (40%), dịch vụ công cộng (30%), năng lượng (30%), giáo dục (30%),... Cho đến hiện tại, phần lớn startup sử dụng Blockchain trong lĩnh vực tài chính.

## **3. Mục đích nghiên cứu**

Project nghiên cứu cách tạo ra một hợp đồng thông minh dựa trên nền tảng Blockchain, từ đó giúp em học thêm được những công nghệ mới, những kiến thức sâu hơn.

Project này sẽ là tiền đề cho đồ án tốt nghiệp của em sau đó.

## **4. Phạm vi nghiên cứu**

Project này tập trung nghiên cứu vào công nghệ chuỗi khối, cách tạo ra các chain, lập trình web bằng template Flask/Jinja2,...

Project được thực hiện trong vòng 6 tuần kể từ khi quyết định đề tài.

## **5. Đóng góp của đề tài**

Em làm đề tài này với hi vọng sẽ giúp người đọc hiểu thêm về công nghệ chuỗi khối cũng như các ứng dụng của nó, để từ đó có thể phục vụ cho quá trình làm việc sau này.

## **6. Kết cấu bài báo cáo**

Ngoài lời cảm ơn, mục lục, lời mở đầu, kết luận và tài liệu tham khảo, bài báo cáo được chia làm 3 phần chính:

Chương 1: Tổng quan về hợp đồng thông minh

Trong chương này, em sẽ làm rõ khái niệm chuỗi khối, hợp đồng thông minh cũng như lợi ích của chúng.

Chương 2: Phân tích project Smart Contract

Trong chương này, em sẽ phân tích chi tiết cách tạo ra một website sử dụng framework Flask để tạo hợp đồng thông minh, phân tích các công nghệ mới đã được sử dụng.

Chương 3: Đánh giá project

Trong chương cuối cùng, em sẽ nêu lên những đánh giá của bản thân về project này cũng như các định hướng phát triển trong tương lai.

# **CHƯƠNG I: TỔNG QUAN VỀ HỢP ĐỒNG THÔNG MINH**

## **1.1. Khái niệm blockchain**

Blockchain là công nghệ chuỗi – khối, cho phép truyền tải dữ liệu một cách an toàn dựa trên hệ thống mã hóa vô cùng phức tạp, tương tự như cuốn sổ cái kế toán của một công ty, nơi mà tiền được giám sát chặt chẽ và ghi nhận mọi giao dịch trên mạng ngang hàng.

Mỗi khối (block) đều chứa thông tin về thời gian khởi tạo và được liên kết với khối trước đó, kèm theo đó là một mã thời gian và dữ liệu giao dịch. Dữ liệu khi đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được. Blockchain được thiết kế để chống lại việc gian lận, thay đổi của dữ liệu.

Công nghệ Blockchain – sự kết hợp giữa 3 loại công nghệ:

Mật mã học: để đảm bảo tính minh bạch, toàn vẹn và riêng tư thì công nghệ Blockchain đã sử dụng public key và hàm hash function.

Mạng ngang hàng: Mỗi một nút trong mạng được xem như một client và cũng là server để lưu trữ bản sao ứng dụng.

Lý thuyết trò chơi: Tất cả các nút tham gia vào hệ thống đều phải tuân thủ luật chơi đồng thuận (giao thức PoW, PoS,…) và được thúc đẩy bởi động lực kinh tế.

## **1.2. Khái niệm hợp đồng thông minh**

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.

Điểm nổi bật nhất của Smart Contract là cho phép hai bên tham gia thực hiện hợp đồng một cách chính xác, an toàn và nhanh chóng; mà không cần các bên biết nhau từ trước, cũng không cần phải gặp trực tiếp để có thể làm việc với nhau, hay một bên trung gian thứ ba mà chỉ cần có kết nối Internet.

Về bản chất, các hợp đồng thông minh trên blockchain cho phép tạo ra các giao thức không cần dựa trên sự tin cậy. Tức là hai bên trong hợp đồng có thể đưa ra các cam kết thông qua blockchain mà không cần phải biết hoặc tin tưởng lẫn nhau. Họ có thể đảm bảo rằng nếu các điều kiện của hợp đồng không được thỏa mãn, hợp đồng sẽ không được thực thi. Ngoài ra, việc sử dụng hợp đồng thông minh loại bỏ nhu cầu đối với các bên trung gian, giúp giảm đáng kể chi phí hoạt động.

## **1.3. Ứng dụng của hợp đồng thông minh**

Smart Contract là một ứng dụng tận dụng tất cả những điểm mạnh của công nghệ Blockchain mang lại vì vậy nó có rất nhiều lợi ích, dưới đây là các lợi ích chính của nó.

Tự động hóa: Quá trình được thực hiện hợp đồng là tự động bằng. Đồng thời bạn chính là người tạo hợp đồng, không còn phải phụ thuộc vào môi giới, luật sư hay bất kì ai khác. Như vậy, nó cũng xóa bỏ những nguy cơ đến từ bên thứ ba

Không bị thất lạc: Tài liệu của bạn được mã hóa trên một cuốn sổ cái chung, có nghĩa là không thể bị thất lạc. Với Blockchain, tất cả những người bạn đều có lưu trữ lại tài liệu của bạn.

An toàn: Blockchain sẽ đảm bản sự an toàn cho tài liệu của bạn. Không một hacker nào có thể đe dọa đến chúng.

Tốc độ: Hợp đồng thông minh sử dụng các ngôn ngữ lập trình, code phần mềm để tự động hóa các điều khoản, tiết kiệm hàng tiếng đồng hồ cho những công việc không cần thiết.

Tiết kiệm: Hợp đồng thông minh tiết kiệm cho bạn hàng đống tiền nhờ xóa bỏ khâu trung gian.

Chính xác: Các hợp đồng tự động không chỉ nhanh và rẻ hơn mà còn tránh được các lỗi thường thấy khi viết giấy tờ.

Ứng dụng của Smart Contract có thể sử dụng được trong nhiều lĩnh vực trong tương lai, hiện tại một số lĩnh vực đã triển khai smart contract bao gồm: Tiền điện tử, logistic, ngân hàng, bất động sản thậm chí là việc bầu cử.

Chuỗi cung ứng trong bất kì doanh nghiệp nào đều là một hệ thống kéo dài và gồm nhiều bộ phận khác nhau. Mỗi bộ phận đều có những công việc nhất định, mà phải làm tuần tự. Và chúng phải được ghi lại để khi xảy ra phát sinh còn biết vấn đề ở đâu

Đây là một quá trình dài hơi và kém năng suất, nhưng với Smart Contract thì mỗi bộ phận tham gia đều có thể theo dõi tiến trình công việc để từ đó hoàn thành nhiệm vụ đúng hạn. Smart contract bảo đảm tính minh bạch trong điều khoản hợp đồng, chống gian lận.

Nó còn có thể cung cấp cho ta khả năng giám sát quá trình cung ứng nếu như được tích hợp chung với Mạng lưới vạn vật kết nối bằng Internet (Internet of Things).

Với Smart Contract thì hồ sơ bệnh lý của người bệnh sẽ được mã hóa và lưu trữ trên Blockchain với một khóa riêng, chỉ những người có khóa đó mới có thể truy cập vào xem hồ sơ được. Đồng thời các hóa đơn cho các cuộc phẫu thuật được lưu trữ trên Blockchain và được tự động chuyển cho bên bảo hiểm. Sổ cái cũng có thể được sử dụng trong việc quản lý chăm sóc y tế, ví dụ như giám sát thuốc men, kết quả xét nghiệm và quản lý các nguồn cung y tế.

## **\*/ Tiểu kết chương 1:**

Trong chương 1, chúng ta đã làm rõ những khái niệm về blockchain nói chung và hợp đồng thông minh nói riêng. 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.

Trong chương 2, ta sẽ cùng tìm hiểu chi tiết cách tạo ra một Smart Contract dựa trên công nghệ chuỗi khối.

# **CHƯƠNG II: PHÂN TÍCH PROJECT SMART CONTRACT**

Project này dừng lại ở việc nghiên cứu những công nghệ mới nên hợp đồng vẫn còn đơn giản. Hợp đồng có các chức năng: Đăng nhập, đăng ký, đào coin, xem chain, tạo hợp đồng, kiểm tra hợp đồng.

## **2.1. Hệ thống Blockchain**

*2.1.1. Cấu trúc một khối*

Mỗi một khối (block) sẽ có index, timestamp, danh sách các giao dịch và proof (sẽ nói chi tiết hơn ở sau) và hash của khối trước. Dưới đây là một khối ví dụ

Graphical user interface, text, application

Description automatically generated

*2.1.2. Thêm mới giao dịch*

Thêm mới giao dịch sẽ tạo một giao dịch và gắn vào “transactions” của khối tiếp theo.

Text

Description automatically generated

*2.1.3. Tạo khối mới*

Khi khởi tạo Blockchain, chúng ta cần phải khởi tạo block genesis, đây là block đầu tiên.

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Cụ thể:

– Hàm new\_block() sẽ tạo ra một block mới và đẩy nó vào trong Blockchain.

– Hàm new\_transaction() tạo ra một giao dịch mới, sau này sẽ được lưu vào Block được đào tiếp theo.

– Hàm hash() để tạo hash cho Block. Cụ thể ở đây sử dụng SHA-256

Text

Description automatically generated

*2.1.4. Proof of Work*

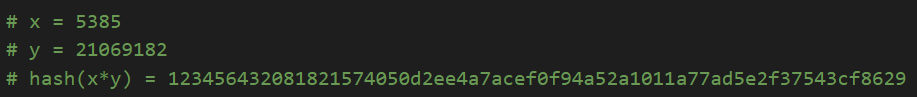
Trước hết hãy nhắc lại về hash. Nó là một cách mã hoá hiểu nôm na như một hàm số. Cho hai đầu vào giống nhau thì sẽ luôn cho ra một kết quả giống nhau. Nhưng nếu có một đầu ra thì rất rất khó để có thể tìm lại được đầu vào.

Bài toán cần tìm hiểu trong phần này là Proof of Work (PoW), nó là cách một khối của Blockchain được đào hoặc được tạo ra. Mục tiêu của chúng ta là tìm ra được lời giải của bài toán (thường là một con số). Tương tự, số đó phải dễ dàng kiểm chứng nhưng rất khó để tìm ra bởi bất cứ ai trong hệ thống.

Giả sử ta có hai số x và y. Bài toán của chúng ta là hash của x\*y phải bắt đầu bởi dãy 123456, cụ thể hash(x\*y) = 123456… x sẽ là một số ngẫu nhiên được khởi tạo trước.

Text

Description automatically generated



Trong bitcoin thì thuật toán Proof of Work này gọi là Hashcash. Và nó cũng tương tự như ví dụ bên trên. Trong thực tế, các tay đào bitcoin phải giải những bài toán phức tạp hơn thế này gấp nhiều lần. Việc một người giải được bài toán thì khó chứ để xác thực là người đó có giải được bài toán hay không thì rất đơn giản. Và để trả công cho người giải được thì người đó sẽ được thưởng một đơn vị tiền qua một giao dịch.

*2.1.5. Cài đặt Proof of Work*

Text

Description automatically generated

Text

Description automatically generated

Bài toán cần giải là: Tìm số p sao cho khi hash(pp') thì 4 ký tự đầu đều là số 0 (p' cho trước-là proof\_of\_work của block trước)

*2.1.6. Xây dựng database*

Database tên project3 có 2 table: user và contract.

Table user sẽ chứa các thông tin của người dùng:

Graphical user interface, application

Description automatically generated

Table contract sẽ chứa các thông tin về hợp đồng được tạo:

Graphical user interface

Description automatically generated

## **2.2. Xây dựng API**

Chúng ta sẽ sử dụng framework Flask để xây dựng nên hệ thống blockchain.

Chúng ta sẽ cài đặt 3 methods chính:

/mine thực hiện đào 1 coin.

/transactions tạo 1 hợp đồng mới cho khối

/chain trả lại toàn bộ Blockchain.

Ngoài ra, ứng dụng còn có các chức năng đăng nhập, đăng ký và kiểm tra xem chain có bị thay đổi hay không

*2.2.1. Đào một coin*

Sau khi đăng nhập vào chương trình, giao diện chính của website sẽ như sau:

Graphical user interface, text, application, email

Description automatically generated

Mỗi một tài khoản sẽ có 1 hash ID của mình chính bằng sha256(username). Ngoài ra còn hiển thị số coin của mình. Khi người dùng muốn đào coin, ấn nút “Mine”, khi đào xong sẽ xuất hiện thông báo đào thành công:

Graphical user interface, application

Description automatically generated

Và số coin sẽ tăng lên

Graphical user interface, text, application, email

Description automatically generated

Tóm lại, hàm mine() sẽ thực thi như sau:

- Tính toán Proof Of Work

- Thưởng cho người thành công 1 đồng tiền

- Tạo ra một block mới và thêm vào chain

*2.2.2. Tạo hợp đồng*

Khi ấn vào Transaction, ta có thể tạo một hợp đồng mới với giao diện sau:

Graphical user interface, application, Teams

Description automatically generated

Recipient là hash ID của người nhận, amount là số coin chuyển đi và Content là nội dung của hợp đồng.

Hash ID phải là một hash ID hợp lệ, nếu không sẽ không thể thực hiện thành công. Ngoài ra, số lượng coin chuyển đi cũng không được nhiều hơn số coin hiện có trong ví.

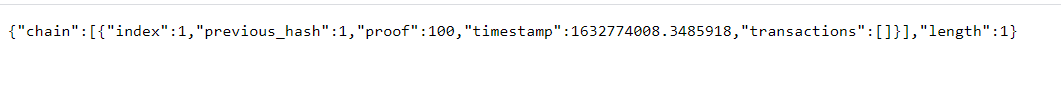
Sau khi tạo hợp đồng, số coin còn lại sẽ được cập nhật

Graphical user interface, text, application, email

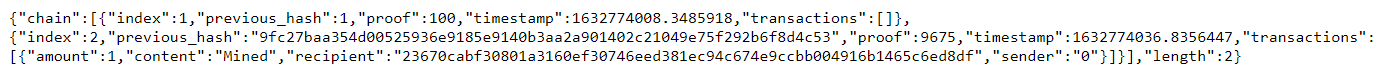
Description automatically generated

*2.2.3. Xem blockchain*

Khi mới khởi tạo, chain sẽ chỉ có một khối khởi tạo như sau

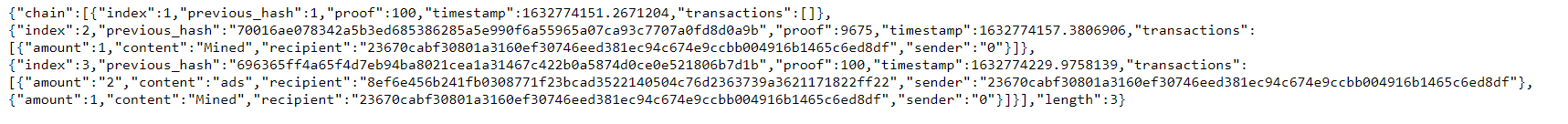


Sau khi có người dùng đào được 1 coin, chain mới sẽ trở thành



Với người nhận là hash ID của người đào, người gửi là 0, và nội dung là “Mined” – đã đào, index là 2.

Khi có một hợp đồng mới được tạo, hợp đồng này sẽ được thêm vào trong khối thứ 3. Cho đến khi có một người đào thêm một khối, hợp đồng sẽ được hiển thị ra thành danh sách. Lúc này sẽ có 2 hợp đồng, gồm người gửi đã tạo trước đó và người đào một coin mới



*2.2.4. Kiểm tra blockchain*

Trong một mạng Blockchain, xung đột xảy ra khi các node trong mạng không có chung một chuỗi Blockchain. Để giải quyết vấn đề này, chúng ta sẽ sử dụng luật chuỗi nào dài nhất là chuối hợp lệ.

Text

Description automatically generated

Text

Description automatically generated

Method valid\_chain() chịu trách nhiệm cho việc kiểm tra một chain có hợp lệ hay không

Method resolve\_conflicts() kiểm tra xem các node trong mạng có hợp lệ hay không. Nếu một chain hợp lệ và dài hơn chain hiện tại thì nó sẽ tiến hành thay thế chain hiện tại.

Ta sẽ thêm 2 API như sau

Text

Description automatically generated

Text

Description automatically generated

Đến đây ta có thể lấy một máy tính khác để tạo thành một node mới, hoặc có thể chạy chương trình trên các cổng khác nhau. Ta sẽ chạy thêm chương trình với cổng 5001, sau đó register.

Graphical user interface, text, application, email

Description automatically generated

Ta đã tạo ra 1 nút mới cùng lưu dữ liệu với nút ban đầu.

Tiến hành đào 1 vài coin tại nút thứ 2, ta kiểm tra thấy nút 2 đã được xác thực

Text

Description automatically generated with medium confidence

Còn tại nút 1 đã được thay thế

A picture containing text

Description automatically generated

## **\*/ Tiểu kết chương 2:**

Trong chương 2, chúng ta đã đi chi tiết cách tạo ra một Hợp đồng thông minh bằng Flask và chạy chương trình. Đây đều là những kiến thức cơ bản trong blockchain và có thể tìm thấy ở trên Internet.

Trong chương 3, ta sẽ đánh giá ưu nhược điểm cũng như những định hướng phát triển của Project trong tương lai.

# **CHƯƠNG III: ĐÁNH GIÁ PROJECT**

## **3.1. Ưu điểm**

Trong một thời gian khá ngắn của học kì hè, Project cũng đã được hoàn thiện phần khung.

Project đã hoàn thành những phần thiết yếu của một hệ thống Smart contract:

- Chỉ thực hiện các hành động mà chúng được thiết kế để thực hiện trong trường hợp các điều kiện được thỏa mãn. Bên cạnh đó, các kết quả của Smart Contract không đổi dù người thực hiện là ai.

- Có thể tự động hóa tất cả các loại tác vụ, nó hoạt động như một chương trình tự thực hiện.

- Không thể sửa đổi Smart Contract sau khi triển khai.

- Trước khi triển khai, Smart Contract có thể được mã hóa theo nhiều cách khác nhau. Vì vậy, chúng có thể được sử dụng để tạo ra nhiều loại ứng dụng phi tập trung.

- Hai hoặc nhiều bên của hợp đồng có thể tương tác thông qua Smart Contract mà không cần biết hoặc tin tưởng lẫn nhau. Ngoài ra, công nghệ blockchain đảm bảo tính chính xác của dữ liệu.

- Vì các Smart Contract dựa trên một blockchain công khai, không ai có thể thay đổi mã nguồn của chúng, mặc dù bất kỳ ai cũng có thể xem được.

## **3.2. Nhược điểm**

Do kiến thức cũng như tư duy còn hạn chế, project mới chỉ hoàn thiện được phần khung sườn. Toàn bộ các chức năng vẫn còn khá sơ sài và chưa được trau chuốt, xử lý từng sự kiện.

Ứng dụng chưa có chức năng phân tán ra các nút mới, và vì thế không thể tạo thành một ứng dụng phi tập trung.

Giao diện website chưa đẹp, cần cải tiến.

## **3.3. Định hướng phát triển**

Hợp đồng thông minh này có thể có rất nhiều hướng phát triển hơn trong tương lai:

Sửa lại giao diện cho đẹp mắt

Tạo ra các nút mới để phân tán, lưu trữ dữ liệu trên nhiều máy chủ.

Hoàn thiện các chức năng và thêm mới:

* **Chủ thể hợp đồng:** Smart Contract phải được cấp khả năng truy cập đến sản phẩm/dịch vụ liệt kê trong hợp đồng để có thể tự động khóa hay mở khóa chúng.
* **Chữ kí điện tử:** Tất cả các bên tham gia vào Smart Contract đều phải đồng ý triển khai thỏa thuận bằng các khóa cá nhân (chữ kí điện tử) của họ.
* **Điều khoản hợp đồng**: Điều khoản trong Smart Contract có dạng là một chuỗi các hoạt động. Và các bên tham gia hợp đồng đều phải ký chấp nhận nó.
* **Nền tảng phân quyền:** Smart Contract sau khi hoàn tất sẽ được tải lên Blockchain của nền tảng phân quyền tương ứng và được phân phối về cho các node của nền tảng ấy.

## **\*/ Tiểu kết chương 3:**

Với các đặc tính của hợp đồng thông minh như đã giới thiệu ở phần trên, chúng ta có thể thấy Smart Contract nói riêng và Blockchain nói chung đem lại rất nhiều lợi ích cho con người. Chúng ta cần có sự hiểu biết về nó để có thể nắm rõ bản chất cũng như áp dụng vào thực tiễn.

# **KẾT LUẬN**

Hợp đồng thông minh - Smart Contract là hợp đồng điện tử hoặc một ứng dụng, chương trình được lập trình bắt buộc để thực hiện các điều khoản của hợp đồng và được thực hiện bởi một bộ quy tắc cụ thể.

Toàn bộ quy trình hoạt động của Hợp đồng thông minh được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài hay thông qua một bên thứ ba nào. 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 Hợp đồng thông minh tương đương với một hợp đồng truyền thống có pháp lý và được ghi lại dưới ngôn ngữ của lập trình.

Điểm nổi bật nhất của Hợp đồng là cho phép hai bên tham gia thực hiện hợp đồng một cách chính xác, an toàn và nhanh chóng; mà không cần các bên phải biết nhau từ trước, cũng không cần phải gặp trực tiếp để có thể trao đổi, ký hợp đồng với nhau, hay một bên trung gian thứ ba mà chỉ cần có kết nối Internet.

Hợp đồng thông minh là một ứng dụng sở hữu tất cả những điểm mạnh của công nghệ Blockchain mang lại vì vậy nó có rất nhiều ưu điểm, lợi ích như: tính tự động hóa, tính chính xác cao, không thể thay đổi, tính bảo mật cao, v.v… Hiện nay, hình thức này cũng đã được thừa nhận tính pháp lý tương đương với hợp đồng giấy nên các doanh nghiệp.

Những cá nhân theo ngành Công nghệ thông tin rất cần hiểu rõ về Smart Contract nói riêng và Blockchain nói chung để có thể góp công sức vào nền phát triển của nước nhà.

# **TÀI LIỆU THAM KHẢO**

1.https://www.investopedia.com/terms/s/smart-contracts.asp#:~:text=A%20smart%20contract%20is%20a,a%20distributed%2C%20decentralized%20blockchain%20network.

2.https://theblockchaintest.com/uploads/resources/WatPy%20-%20Building%20Smart%20Contract%20Applications%20Python,%20Solidity,%20Flask%20-%202019%20-%20Sep.pdf

3.https://www.innoplexus.com/blog/how-to-develop-ethereum-contract-using-python-flask/

4.https://developpaper.com/python-and-flask-framework-to-develop-ethernet-smart-contract/

5. https://stackoverflow.com/

# **PHỤ LỤC**

**Một số hàm mới được sử dụng trong code và thư viện:**

|  |  |
| --- | --- |
| **Thư viện** | **Hàm** |
| windows.h | WinMain(),SetWindowsHookEx(),  CallNextHookEx(),  UnhookWindowsHookEx() |
| string.h | ToUnicode() |