 ĐẠI HỌC BÁCH KHOA HÀ NỘI

TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

──────── \* ────────

Ảnh có chứa văn bản, áp phích, Phông chữ, Đồ họa

Mô tả được tạo tự động

BÁO CÁO BLOCKCHAIN

ĐỀ TÀI: XÂY DỰNG HỆ THỐNG PHI TẬP TRUNG TƯƠNG TỰ SPLITWISE VÀ UNISWAP

Giảng viên hướng dẫn: Ts. Nguyễn Bình Minh

Nhóm sinh viên thực hiện: Nhóm 9

*Trần Đức Hải - 20194270*

*Nguyễn Phương Nam - 20194336*

*Nguyễn Mạnh Duy - 20194362*

Nội dung

[Phân công công việc 3](#_Toc139988885)

[I. Giới thiệu bài toán 4](#_Toc139988886)

[1. Blockchain Splitwise 4](#_Toc139988887)

[2. Blockchain Uniswap 4](#_Toc139988888)

[II. Cơ sở lý thuyết 5](#_Toc139988889)

[1. Nền tảng công nghệ 5](#_Toc139988890)

[a. Blockchain 5](#_Toc139988891)

[b. Smart contract 6](#_Toc139988892)

[c. ERC-20 6](#_Toc139988893)

[2. Blockchain Splitwise 7](#_Toc139988894)

[a. Vòng lặp giải quyết nợ nần 7](#_Toc139988895)

[b. Thuật toán tìm kiếm theo chiều rộng 8](#_Toc139988896)

[3. Bockchain Uniswap 9](#_Toc139988897)

[b. Giao dịch trên hệ thống Swap token 9](#_Toc139988898)

[c. Trượt giá (Slippage) 12](#_Toc139988899)

[III. Xây dựng hệ thống 13](#_Toc139988900)

[1. Blockchain Splitwise 13](#_Toc139988901)

[a. Tạo Smart Contract 13](#_Toc139988902)

[b. Tương tác với Smart contract qua giao diện 15](#_Toc139988903)

[2. Blockchain Uniswap 17](#_Toc139988904)

[a. Tạo smart contract custom token 17](#_Toc139988905)

[c. Tương tác Smart contract qua giao diện 19](#_Toc139988906)

[IV. Kiểm thử và đánh giá 21](#_Toc139988907)

[1. Blockchain Splitwise 21](#_Toc139988908)

[2. Blockchain Uniswap 22](#_Toc139988909)

[a. Khi giao dịch 22](#_Toc139988910)

[b. Khi người cung cấp muốn cung cấp thanh khoản 23](#_Toc139988911)

[c. Khi người cung cấp muốn rút thanh khoản 24](#_Toc139988912)

[c. Khi người cung cấp muốn rút hết thanh khoản 25](#_Toc139988913)

[IV. Kết luận 26](#_Toc139988914)

# Phân công công việc

|  |  |
| --- | --- |
| Tên | Công việc thực hiện |
| Trần Đức Hải | Xây dựng smart contract và các hàm tương người dùng tác bài 1 – mô phỏng splitwise |
| Nguyễn Phương Nam | Xây dựng 2 smart contract token và exchange giao dịch bài 2 – mô phỏng uniswap |
| Nguyễn Mạnh Duy | Xây dựng các hàm tương tác người dùng bài số 2 – mô phỏng uniswap |

Source Code:

Project1:

<https://github.com/NBlue/blockchain_project/tree/master/Project1/StarterCode>

Project2: <https://github.com/NBlue/blockchain_project/tree/master/Project2/CS251_Dex_V2_Starter>

# I. Giới thiệu bài toán

## 1. Blockchain Splitwise

Splitwise là một ứng dụng quản lý các khoản nợ và trả nợ phổ biến, giúp nhóm người dùng chia sẻ các khoản chi tiêu và tính toán tổng cộng các khoản nợ/phải trả giữa các thành viên. Đối với hệ thống mà nhóm đang đề cập trong bài toán là một phiên bản blockchain của Splitwise, với mục đích đơn giản hóa quá trình theo dõi ai nợ ai bao nhiêu tiền trong một nhóm người. Sử dụng công nghệ blockchain để tạo ra một hệ thống đáng tin cậy mà không phải dựa vào một bên trung gian.

Bằng cách xây dựng một blockchain tương tự Splitwise, ứng dụng cung cấp một phương pháp an toàn và minh bạch để ghi lại các khoản nợ và trả nợ giữa các thành viên. Mọi giao dịch và thông tin liên quan đến nợ được lưu trữ trên blockchain, cho phép tất cả các thành viên trong nhóm có thể truy cập và xem thông tin này một cách công khai. Do đây là một mạng lưới phân tán mà không cần phải tin tưởng vào một bên thứ ba trung gian. Mỗi thành viên trong nhóm đều có quyền kiểm tra và xác minh các giao dịch trên blockchain, đảm bảo tính toàn vẹn và không thể thay đổi của dữ liệu.

Hơn nữa, việc sử dụng blockchain cũng mang lại tính minh bạch cao. Mọi thông tin về các khoản nợ và trả nợ được ghi lại một cách rõ ràng và không thể thay đổi. Điều này giúp tránh tranh chấp và bất đồng trong việc xác định số tiền mà mỗi thành viên phải trả. Mỗi thành viên có thể dễ dàng kiểm tra lịch sử giao dịch và số dư của mình trên blockchain, đảm bảo rằng mọi thông tin đều công bằng và minh bạch.

## 2. Blockchain Uniswap

Trong thời đại kỹ thuật số ngày nay, việc tạo ra các hệ thống trao đổi tiền điện tử phi tập trung đã trở thành một xu hướng quan trọng trong lĩnh vực blockchain. Điều này cho phép người dùng trao đổi các tài sản kỹ thuật số một cách thuận tiện và an toàn, mà không cần sự can thiệp của các bên trung gian truyền thống.

Dựa trên cơ sở đó, nhóm muốn xây dựng một hệ thống trao đổi tiền điện tử phi tập trung, với mục tiêu cung cấp các chức năng tương tự như sàn giao dịch Uniswap. Uniswap đã trở thành một trong những sàn giao dịch phi tập trung hàng đầu trên nền tảng Ethereum, nổi tiếng với tính năng tự động hoá quy trình giao dịch và sự công bằng trong việc cung cấp thanh khoản.

Hệ thống sẽ cho phép người dùng trao đổi tài sản kỹ thuật số với nhau một cách trực tiếp và an toàn. Chúng tôi nhắm đến việc tạo ra một giao diện người dùng thân thiện và dễ sử dụng, mô phỏng cho phép người dùng truy cập và thực hiện các giao dịch một cách nhanh chóng và tiện lợi. Tuy bài toán này để phục vụ mục đích học tập nhưng vẫn đảm bảo tính an toàn và bảo mật cho người dùng.

Trong báo cáo này, nhóm sẽ trình bày chi tiết về kiến trúc, chức năng và các kỹ thuật quan trọng trong việc xây dựng hệ thống trao đổi tiền điện tử phi tập trung tương tự như Uniswap. Nhóm cũng sẽ trình bày về quy trình triển khai và các thử nghiệm đã được tiến hành để đánh giá tính ổn định và hiệu suất của hệ thống.

# II. Cơ sở lý thuyết

## 1. Nền tảng công nghệ

### a. Blockchain

Blockchain là một sổ cái kỹ thuật số được phân chia. Hiểu đơn giản là một cuốn sổ ghi ghép lại mọi thứ sinh ra và mất đi, sau đó cuốn sổ đó được sao chép cho mỗi người tham gia vào mạng giữ một bản. Điều này cho thấy rằng trong toàn bộ hệ thống không phải chỉ có một vị trí duy nhất, một tài liệu có thể làm căn cứ đáng tin (authority) duy nhất, vì những lần sao chép cùng một phiên bản sổ cái được đặt ở nhiều nơi.

Tất cả các bản sao này được cập nhật khi dữ liệu hoặc giao dịch mới được ghi vào blockchain thông qua sự đồng thuận của tất cả mọi người tham gia. Một số người trong hệ thống có trách nhiệm phê duyệt các giao dịch và giám sát mạng bằng cách giải quyết các công thức tinh vi với sự trợ giúp của máy tính hoặc nắm giữ một số lượng lớn token. Nó là một hệ thống ngang hàng P2P, loại bỏ tất cả mọi khâu trung gian, làm tăng cường an ninh, minh bạch và sự ổn định cũng như giảm thiểu chi phí và lỗi do con người gây ra.

Bằng cách cho phép phân chia dữ liệu cho số đông khiến cho chúng không thể bị chỉnh sửa, phá hoại hay thao túng, công nghệ blockchain đã tạo ra xương sống cho một loại hình Internet mới.

Blockchain được dùng để lưu trữ thông tin trong các khối thông tin được liên kết với nhau. Nó được quản lý bởi tất cả mọi người tham gia hệ thống. Thay vì một bên thứ 3 riêng lẻ như nhà nước hay ngân hàng trung ương. Đồng thời cho phép truyền tải dữ liệu một cách an toàn bằng một hệ thống mã hóa phức tạp, và được mở rộng theo thời gian. Hơn nữa, công nghệ này được tạo ra để chống lại sự thay đổi dữ liệu trong hệ thống. Nó cũng có một tính năng rất đặc biệt đó là việc truyền tải dữ liệu không đòi hỏi một trung gian nào để xác nhận thông tin.

Bởi vì trong hệ thống Blockchain tồn tại rất nhiều nút hoạt động độc lập có khả năng xác thực các thông tin trong hệ thống mà không đòi hỏi “dấu hiệu của niềm tin”. Thông tin khi được nhập vào trong chuỗi khối blockchain thì sẽ không thể thay đổi và chỉ được bổ sung thêm khi có sự chấp thuận của tất cả mọi người trong hệ thống.

Nhất là các dữ liệu nhạy cảm như tài khoản ngân hàng online, tài khoản thẻ thanh toán… Ngay cả khi nếu một phần của hệ thống blockchain bị tấn công, thì các phần khác không bị ảnh hưởng và vẫn tiếp tục hoạt động để bảo vệ thông tin

Ảnh có chứa biểu đồ, khối lập phương

Mô tả được tạo tự động

### b. Smart contract

Smart contract là một chương trình viết bằng ngôn ngữ lập trình (như Solidity trên Ethereum) và được lưu trữ trên blockchain. Nó chứa các quy tắc và điều kiện mà các bên tham gia phải tuân thủ và tự động thực thi các giao dịch dựa trên các điều khoản đã được định nghĩa.

Smart contract tự động xác thực và thực thi các điều khoản mà nó chứa. Nó hoạt động theo cách không thể thay đổi và không thể bị can thiệp từ bất kỳ bên nào ngoại trừ các bên tham gia ban đầu.

Smart contract giúp xây dựng các ứng dụng phi tập trung, nơi các bên không cần phải tin tưởng vào một bên thứ ba. Nó cung cấp tính minh bạch, an toàn và giảm thiểu sự phụ thuộc vào trung gian.

Smart contract bao gồm các thành phần như biến, hàm, modifier, event và inheritance. Biến được sử dụng để lưu trữ dữ liệu, hàm để thực hiện các tác vụ, modifier để thay đổi hành vi của hàm, event để ghi lại các sự kiện và inheritance để kế thừa các tính năng từ các hợp đồng khác.

Smart contract là hợp đồng thông minh có nhiều ưu điểm so với hợp đồng truyền thống được giao kết bằng phương tiện điện tử và sẽ có chữ ký điện tử. Trong khi hợp đồng truyền thống giao kết bằng phương tiện “giấy tờ”, “vật chất” và ký tay sau khi các bên gặp và trao đổi với nhau. So với hợp đồng truyền thống, việc lưu trữ hợp đồng thông minh dễ dàng hơn. Thay vì lưu trữ hợp đồng giấy như thông thường, hợp đồng thông minh sẽ được lưu trữ trực tiếp trên các nền tảng số, không lo thất lạc, hư hỏng.

### c. ERC-20

ERC-20 (Ethereum Request for Comment 20) là một chuẩn tiêu chuẩn của Ethereum được đề xuất bởi Fabian Vogelsteller vào năm 2015. Đây là chuẩn giao thức thông minh thông qua hợp đồng thông minh trên Ethereum, cho phép tạo ra và quản lý các mã thông báo (token) trên mạng blockchain.

ERC-20 đã trở thành chuẩn giao thức phổ biến nhất cho việc tạo mã thông báo trên Ethereum, và nó đã được sử dụng rộng rãi cho việc phát hành các token tiền điện tử, trong đó có cả các dự án ICO (Initial Coin Offering) và các dự án DeFi (Decentralized Finance). Chuẩn ERC-20 định nghĩa một tập hợp các phương thức và sự kiện mà các mã thông báo phải tuân theo để có thể tương tác và hoạt động một cách chuẩn mực trên blockchain Ethereum.

Một trong những điểm đáng chú ý của chuẩn ERC-20 là tính tương thích và sự tương tác giữa các mã thông báo. Điều này cho phép các mã thông báo ERC-20 được giao dịch và sử dụng trong các ứng dụng, ví điện tử và sàn giao dịch mà không cần triển khai một hợp đồng thông minh riêng cho mỗi loại mã thông báo. Điều này đơn giản hóa việc tích hợp và tương tác với các ứng dụng và hệ thống khác trên blockchain Ethereum.

Chuẩn ERC-20 định nghĩa các phương thức cơ bản như “totalSupply()” để truy vấn tổng nguồn cung của mã thông báo, “balanceOf(address)” để truy vấn số lượng mã thông báo đang nắm giữ bởi một địa chỉ cụ thể, “transfer(address, uint256)” để chuyển mã thông báo từ một địa chỉ này sang một địa chỉ khác, và các phương thức khác như “approve(address, uint256)” để ủy quyền một số lượng mã thông báo cho một địa chỉ thứ ba và “transferFrom(address, address, uint256)” để chuyển mã thông báo từ một địa chỉ đã được ủy quyền.

Các dự án xây dựng hệ thống trao đổi tiền điện tử phi tập trung, như Uniswap, thường tận dụng chuẩn ERC-20 để triển khai các mã thông báo và cho phép giao dịch trên nền tảng của họ. Điều này tạo ra sự linh hoạt và khả năng tương tác với một loạt các ứng dụng và dịch vụ khác trong hệ sinh thái Ethereum.

## 2. Blockchain Splitwise

### a. Vòng lặp giải quyết nợ nần

Đối với hệt thống Splitwise hiểu đơn giản là bài toán ai nợ tiền ai.Ví dụ bài toán nợ tiền xảy ra giữa các thành viên Carol, Bob và Alice. Alice đang nợ Bob 10$, Bob đang nợ Carol 10$ đã được ghi nợ trên blockchain. Trong buổi đi ăn giữa Carol và Bob, khi Carol trả tiền cho bữa ăn của cô và Bob, cô có thể yêu cầu Bob gửi một hợp đồng nợ (IOU), và cô có thể xác minh rằng anh ta đã làm như vậy. Việc lưu trữ công khai trên blockchain sẽ phục vụ như một nguồn thông tin duy nhất cho việc ai nợ ai. Sau đó xuất hiện 1 chu trình nợ giữa Carol, Bob và Alice. Khi chu trình nợ được giải quyế, Carol sẽ thấy rằng Bob không còn nợ cô tiền nữa.

Tóm lại khi một người mượn ai đó 1 khoản tiền, ta có thể xem IOUs như là một đồ thị nợ. Tức là, giả sử mỗi người dùng là một nút, và mỗi cạnh có trọng số từ A đến B với trọng số X đại diện cho việc 'A nợ $X cho B'. Chúng ta sẽ viết thành A −!X B. Ứng dụng của chúng ta muốn 'giải quyết' bất kỳ chu trình nào trong đồ thị này bằng cách trừ đi giá trị nhỏ nhất trong chu trình đó từ mỗi bước trong chu trình (điều này sẽ làm cho ít nhất một bước trong chu trình có trọng số '0').

Ví dụ, nếu A −!15 B và B −!11 C, khi C thêm C −!16 A, các số dư thực tế sẽ được cập nhật để phản ánh rằng A −!4 B, B −!0 C và C −!5 A.

Ảnh có chứa xe đạp, bản phác thảo

Mô tả được tạo tự động

Tương tự, nếu C thêm C −!9 A, các số dư thực tế sẽ được cập nhật để phản ánh rằng A −!6 B, B −!2 C và C −!0 A.

Ảnh có chứa biểu đồ, vòng tròn, bản phác thảo, thiết kế

Mô tả được tạo tự động

### b. Thuật toán tìm kiếm theo chiều rộng

Để giải quyết vòng lặp nợ nần trong hệ thống này, nhóm đã sử dụng thuật toán tìm kiếm theo chiều rộng (BFS - Breadth-First Search). Thuật toán BFS là một thuật toán quan trọng trong lĩnh vực truyền thông và xử lý đồ thị, nó cho phép chúng ta khám phá các đỉnh của đồ thị một cách hệ thống từ đỉnh gốc.

Trong ngữ cảnh của hệ thống trao đổi tiền điện tử phi tập trung, thuật toán BFS được sử dụng để xác định các chuỗi giao dịch có khả năng gây ra vòng lặp nợ nần. Khi người dùng thực hiện một giao dịch mới trên hệ thống (tức là khi thêm 1 IOU), hệ thống sẽ kiểm tra xem liệu giao dịch đó có tạo ra một vòng lặp nợ nần hay không.

Thuật toán BFS bắt đầu bằng việc đặt đỉnh gốc là giao dịch mới nhất và tiến hành duyệt qua các giao dịch liên quan trực tiếp đến giao dịch gốc này. Hệ thống sẽ duyệt qua tất cả các đỉnh lân cận của đỉnh gốc trước khi tiếp tục duyệt các đỉnh còn lại trên đồ thị giao dịch. Quá trình này được thực hiện một cách lặp đi lặp lại cho đến khi tất cả các giao dịch đã được kiểm tra. Ta có ví dụ đồ thị như sau:

Ảnh có chứa bản phác thảo, hình vẽ, vòng tròn, biểu đồ

Mô tả được tạo tự động

Khi xuất phát từ A, các đỉnh con của A là B, F. Tiếp tục duyệt các nút con B là C, D, H và của F là G. Các đỉnh C, D không liên kết tới đỉnh nào, đỉnh H liên kết tới G nhưng đỉnh G đã được duyệt trước đó. Và đỉnh G sẽ có con là E. Từ ví dụ này, nếu E nợ A (tức là sẽ thêm 1 IOU lên hệ thống) thì sẽ tạo ra 1 chu trình giữa A, F, G, E.

Khi duyệt qua các giao dịch, hệ thống sẽ kiểm tra xem một giao dịch mới có tạo ra một chuỗi giao dịch tạo thành vòng lặp nợ nần hay không. Nếu phát hiện một vòng lặp nợ nần, hệ thống sẽ áp dụng phương pháp xử lý đã đề cập bên trên để xóa bỏ vòng lặp nợ nần.

Thuật toán tìm kiếm theo chiều rộng (BFS) đã được chúng tôi lựa chọn vì nó cho phép chúng tôi kiểm tra toàn bộ các giao dịch liên quan và xác định vòng lặp nợ nần một cách hiệu quả. Nó giúp chúng tôi tăng tính khả thi và hiệu suất của quy trình kiểm tra và ngăn chặn vòng lặp nợ nần trong hệ thống trao đổi tiền điện tử phi tập trung mà chúng tôi xây dựng.

## 3. Bockchain Uniswap

Uniswap là giao thức hoạt động trên Ethereum để trao đổi token. Không giống như hầu hết các sàn giao dịch được tạo ra và sẽ tính phí giao dịch, Uniswap hoạt động vì mục đích cộng đồng, là công cụ để cộng đồng giao dịch token mà không phải trả phí nền tảng hoặc người trung gian. Bất kỳ token nào cũng có thể được list vào Uniswap bằng cách cung cấp một nguồn vốn bằng ETH và token ERC20 đang được giao dịch.

Trong phạm vi của nhóm là tạo ra một hệ thống trao đổi tiền điện tử phi tập trung với nhiều chức năng tương tự như sàn giao dịch Uniswap. Ngoài ra hệ thống tạo token ERC-20 của riêng mình để mô phỏng 1 hệ thống uniswap hoàn chỉnh có thể trao đổi giữa ETH với ERC-20 token.

a. Bể thanh khoản Liquidity Pool

Bể thanh khoản là một quỹ tài sản được tạo ra bởi các nhà cung cấp thanh khoản (liquidity providers). Hai loại tiền tệ kỹ thuật số được gọi là "Token A" và "Token B" được gửi vào bể thanh khoản theo một tỷ lệ cố định. Ví dụ, nếu một nhà cung cấp thanh khoản muốn thêm 1 ETH và 1000 Token X vào bể thanh khoản, họ sẽ gửi 1 ETH và 1000 Token X vào bể với tỷ lệ 1:1000.

Bể thanh khoản này là nơi mà các giao dịch trao đổi giữa hai loại tiền tệ này diễn ra. Khi người dùng muốn hoán đổi Token A sang Token B (hoặc ngược lại), họ sẽ gửi một số lượng tiền tệ vào bể thanh khoản tương ứng với giá trị muốn hoán đổi. Số lượng tiền tệ này sẽ được lấy ra từ bể thanh khoản và người dùng sẽ nhận lại một số lượng tiền tệ khác từ bể, dựa trên tỷ lệ cung cấp thanh khoản hiện có trong bể.

Tỷ giá hoán đổi giữa hai loại tiền tệ được xác định bằng một công thức tổng quát được gọi là "công thức tổng kết tỷ lệ (Constant Product Formula)" hoặc "x \* y = k". Trong công thức này, x và y đại diện cho số lượng Token A và Token B có sẵn trong bể thanh khoản, và k là một hằng số. Khi người dùng thực hiện một giao dịch, số lượng tiền tệ mà họ gửi vào bể thanh khoản sẽ làm thay đổi giá trị của k, từ đó xác định số lượng tiền tệ mà họ nhận lại từ bể.

Bằng cách có sẵn bể thanh khoản có thể tạo ra một mô hình giao dịch phi tập trung tự động và công bằng. Điều này cho phép người dùng trao đổi các loại tiền tệ kỹ thuật số một cách trực tiếp và thuận tiện, mà không cần phải dựa vào sàn giao dịch trung gian. Bể thanh khoản giúp đảm bảo tính sẵn sàng và đủ thanh khoản cho các giao dịch được thực hiện trên hệ thống.

### b. Giao dịch trên hệ thống Swap token

Một sàn giao dịch phi tập trung bao gồm hai loại người tham gia: nhà cung cấp thanh khoản (Liquidity Provider) và người giao dịch (Swaper). Đối với một cặp giao dịch giữa hai loại token, nhà cung cấp thanh khoản cung cấp một số lượng tương đương của cả hai loại thanh khoản (trong trường hợp này là ETH và token của bạn). Khi người giao dịch hoán đổi giữa hai loại tiền tệ này, họ sẽ thêm một số lượng tiền tệ vào nhóm thanh khoản và nhận được một giá trị tương đương của loại tiền tệ khác từ nhóm thanh khoản. Tỷ giá hoán đổi giữa hai loại tiền tệ được xác định bằng công thức tổng quát: x \* y = k.

Từ công thức trên, ta có công thức để tính phí hoán đổi là:

Ta có là lượng token mà chúng ta sẽ nhận được khi hoán đổi một lượng tương đương khác. Với là lượng token chúng ta muốn đổi. Với công thức trên và giả sửa trong bể thanh khoản ban đầu có 100 Token X và 100 Token Y, ta có bảng hoán đổi sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Lượt | Token X (Pool) | Token Y (Pool) | Đổi X | Nhận Y | Tổng Y nhận |
| 1 | 100 | 100 | 10 | 9.090909 | 9.090909 |
| 2 | 110 | 90.90909 | 10 | 7.575758 | 16.66667 |
| 3 | 120 | 83.33333 | 10 | 6.410256 | 23.07692 |
| 4 | 130 | 76.92308 | 10 | 5.494505 | 28.57143 |
| 5 | 140 | 71.42857 | 10 | 4.761905 | 33.33333 |
| 6 | 150 | 66.66667 | 10 | 4.166667 | 37.5 |
| 7 | 160 | 62.5 | 10 | 3.676471 | 41.17647 |
| 8 | 170 | 58.82353 | 10 | 3.267974 | 44.44445 |
| 9 | 180 | 55.55556 | 10 | 2.923977 | 47.36842 |
| 10 | 190 | 52.63158 | 10 | 2.631579 | 50 |

Qua đây ta có biểu đồ thể hiện sau 10 lần hoãn đổi token X sang token Y (mỗi lần 10 token) sau: Ảnh có chứa văn bản, hàng, Sơ đồ, ảnh chụp màn hình

Mô tả được tạo tự động

Từ điều này ta có thể thấy khi trao đổi token từ nhóm thanh khoản, thì lượng token X và token Y tổng bển thanh khoản sẽ thay đổi theo một đường cong ánh xạ (Trong ví dụ này thì bể pool ban đầu có 100 token x và 100 token y):

Ảnh có chứa văn bản, hàng, biểu đồ, Sơ đồ

Mô tả được tạo tự động

Như chúng ta đã thấy ở trên, việc hoán đổi token X lấy token Y và ngược lại sẽ thay đổi số tiền trong Pool và thay đổi số token sẽ nhận được cho lần hoán đổi tiếp theo. Mỗi lần hoán đổi sẽ di chuyển chúng ta dọc theo đường cong tỷ lệ XY và do đó, mỗi lần hoán đổi tiếp theo sẽ bắt đầu tại nơi mà lần hoán đổi trước đó kết thúc và do đó đưa ra các giá trị khác nhau cho lần hoán đổi.

Một cách khác để thấy điều này là thông qua giá token. Giá token thường được đo bằng cách lấy số token này chia cho số token kia. Cụ thể, nếu muốn tính giá của token Y liên quan đến token X , chúng ta thực hiện điều đó thông qua phép chia X cho Y ( X/Y ). Các giá trị từ sự phân chia này được vẽ trên biểu đồ bên dưới:

Ảnh có chứa hàng, Sơ đồ, biểu đồ, văn bản

Mô tả được tạo tự động

Qua biểu đồ này, chúng ta có thể thấy rõ, khi ta càng hoán đổi nhiều token X để lấy token Y (tức là di chuyển dọc theo đường cong màu xanh sang phải) sẽ làm giá của token Y càng cao. Nghĩa là trong bể thanh khoản đang tăng dần số lượng token X và giảm dần số lượng token Y, điều ngày làm cho giá của token Y so với token X sẽ tăng lên.

### c. Trượt giá (Slippage)

Trượt giá là một giá trị phần trăm mô tả chênh lệch phần trăm giữa các token mà chúng ta sẽ nhận được từ một giao dịch và các token mà chúng ta sẽ nhận được nếu không có trượt giá.

Ảnh có chứa văn bản, hàng, biểu đồ, Sơ đồ

Mô tả được tạo tự động

Tiếp tục biểu đồ giả sử ban đầu với bể thanh khoản đang chứa 100 token X và 100 token Y với tỉ lệ 1:1. Bây giờ, nếu chúng ta muốn trao đổi 100 token X thông qua nhóm thanh khoản này. Ta có thể kiểm tra đường màu xanh trên đồ thị và có thể dễ dàng thấy được sau khi hoán đổi sẽ nhận được 50 token Y. Điều này hoàn toàn đúng khi áp dụng công thức phía trên, ta có:

Do đó, ta đã đổi 100 token X được 50 token Y. Nếu không trược giá, thì với tỉ lệ 1:1 ban đầu, ta có thể đổi 100 token X được 100 token Y. Điều này có nghĩa là chúng ta nhận được ít hơn 50% so với lượng token dự kiến mà ta có thể nhận được, và đó là sự trượt giá khi đổi 100 token X. Công thức tính độ trượt giá với PE là lượng token dự kiến có thể nhận được, AE là lượng token thực tế nhận được:

# III. Xây dựng hệ thống

## 1. Blockchain Splitwise

Dự án có hai thành phần chính: một hợp đồng thông minh, được viết bằng Solidity và chạy trên blockchain, và một client chạy cục bộ trên trình duyệt web, theo dõi blockchain bằng thư viện ethers.js và có thể gọi các hàm trong smart contract.

### a. Tạo Smart Contract

Định nghĩa cấu trúc lưu trữ thông tin khi người dùng thêm 1 IOU – Người dùng mượn tiền và nợ ai đó bao nhiêu tiền. Các thông tin được lưu trữ là: địa chỉ người mượn (debtor), địa chỉ người cho mượn (creditor), số tiền đã mượn (amount), thời gian mượn (timestamp).

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Hàm “add\_IOU(address creditor, uint32 amount, ...)” được sử dụng để người dùng gửi thông báo cho smart contract rằng đã mượn ai đó một khoản tiền:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Hàm “lookup(address debtor, address creditor) public view returns (uint32 ret)” để lấy ra số nợ của 1 địa chỉ:

Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động

Khi có 1 vòng lặp nợ nần (nghĩa là xác nhận có 1 chu trình như đã đề cập bên trên) thì sẽ gọi tới hàm OwnFor sau đây để giải quyết vòng lặp nợ nần:



Ngoài ra còn có các hàm lấy ra thời gian mượn tiền hoặc được mượn tiền mới nhát của 1 địa chỉ và hàm lấy ra tổng nợ hoặc được mượn mới nhất của 1 địa chỉ:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

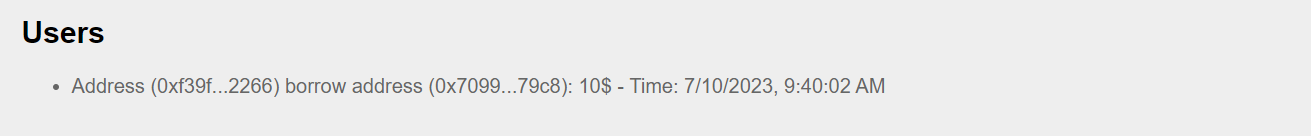
Mô tả được tạo tự động

### b. Tương tác với Smart contract qua giao diện

Lấy ra thông tin tất cả những địa chỉ mượn tiền và cho mượn tiền trong hệ thống:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động



Lấy ra tổng nợ và thời gian tương tác của một địa chỉ trong hệ thống:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, thiết kế

Mô tả được tạo tự động

Khi 1 địa chỉ mượn tiền sẽ gọi đến hàm “add\_IOU” để thêm 1 khoản nợ lên hệ thống. Trong quá trình thêm, hệ thống sẽ tự động kiểm tra liệu có xuất hiện một chu tình nợ không và sẽ tiến hành xử lý chu trình nợ đó:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

## 2. Blockchain Uniswap

Hệ thống sẽ gồm 3 thành phần chính gồm 2 smart contract là “token.sol” (để tạo ra một custom token theo chuẩn ERC-20 và “exchange.sol” để thực hiện các logic giao dịch trong hệ thống. Web\_app để tương tác với người dùng.

### a. Tạo smart contract custom token

Token được tạo theo chuẩn ERC-20. Token này được đặt tên là “Duhana Token” và có kí hiệu là “DHN”:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

b. Tạo smart contract triển khai các chức năng của sàn giao dịch

Hệ thống gồm các chức năng cơ bản cho sàn giao dịch token. Sàn giao dịch này được mô phỏng theo Uniswap V1. Sàn giao dịch chỉ cho phép hoán đổi giữa DHN( token đã được khởi tạo bên trên) và ETH thử nghiệm.

Tại smart contract này sẽ sử dụng địa chỉ smart contract token vừa mới được tạo bên trên. Contract này lưu trữ tỉ lệ phí chuyển khoản là 0.03%; với một bể thanh khoản được lưu trữ với “token\_reserve– Custom token” và “eth\_reserve – ETH”.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

*Các hàm tương tác với bể thanh khoản:*

Hàm “function addLiquidity() external payable” để thêm thanh khoản vào nhóm thanh khoản nếu nhà cung cấp có đủ ETH và token (nếu không, giao dịch sẽ thất bại). Người gọi sẽ gửi ETH vào hợp đồng, có thể truy cập bằng cách sử dụng msg.value. Hàm này cũng sẽ chuyển số lượng tương ứng của token dựa trên tỷ giá hoán đổi hiện tại từ địa chỉ của người gửi đến hợp đồng. Giao dịch sẽ thất bại nếu số dư của nhà cung cấp không đủ.

Hàm “function removeLiquidity(uint amountETH) public payable” để rút một lượng thanh khoản cụ thể từ bể thanh khoản (nếu nhà cung cấp được phép rút số lượng thanh khoản đó) và cập nhật trạng thái của sàn giao dịch tương ứng. Hàm sẽ thất bại nếu người dùng cố gắng rút nhiều hơn số lượng thanh khoản mà họ được phép, hoặc nếu họ cố gắng làm cạn dự trữ ETH hoặc token thành 0.

Hàm “function removeAllLiquidity() external payable” để rút số lượng thanh khoản tối đa mà người gửi được phép rút và cập nhật trạng thái của sàn giao dịch tương ứng. Hàm này sẽ thất bại nếu nhà cung cấp thanh khoản làm cạn dự trữ ETH hoặc token thành 0.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

*Các hàm thực hiện giao dịch giữa hai token:*

Hàm “function swapTokensForETH(uint amountTokens) external payable” để đổi số lượng token cho giá trị tương đương của ETH và cập nhật trạng thái của sàn giao dịch tương ứng. Nếu nhà cung cấp không có đủ token để thực hiện giao dịch, giao dịch sẽ thất bại.

Hàm “function swapETHForTokens() external payable” để đổi số lượng ETH cho giá trị tương đương của token và cập nhật trạng thái của sàn giao dịch tương ứng.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

## c. Tương tác Smart contract qua giao diện

Lấy ra thông tin bể thanh khoản của hệ thống gồm tỉ giá và số lượng token hiện tại trong bể thanh khoản.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình

Mô tả được tạo tự động

Các nhà cung cấp thanh khoản có thực hiện thêm hoặc rút thanh khoản:

Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

Người sử dụng có thể gọi tới các hàm để thực hiện các hoán đổi ETH sang Token hoặc Token sang ETH.

Ảnh có chứa văn bản, Phông chữ, hàng, ảnh chụp màn hình

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

# IV. Kiểm thử và đánh giá

## 1. Blockchain Splitwise



Trong trường hợp khi thêm 1 IOU và tạo ra nhiều chu trình. Hệ thống tự động sử dụng BFS (Thuật toán tìm kiếm theo chiều rộng) và tìm được 1 chu trình bất kì để xử lý. Hệ thống có thể thông báo cho người dùng biết về khoản nợ sẽ được xử lý đối với những địa chỉ tạo ra 1 chu trình:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, phần mềm

Mô tả được tạo tự động

Sau khi phát hiện chu trình nợ nần, hệ thống tự động xử lý và cập nhật lại nợ mới của các địa chỉ:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Mô tả được tạo tự động

## 2. Blockchain Uniswap

### a. Khi giao dịch

Người sử dụng khi muốn thực hiện giao dịch chuyển đổi token trong trường hợp vượt quá mức độ trượt giá cho phép và trong trường hợp thành công:

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Thông tin bể thanh khoản và tỉ giá sau 2 lần hoán đổi 100ETH:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, đại số

Mô tả được tạo tự động

### b. Khi người cung cấp muốn cung cấp thanh khoản

Khi nhà cung cấp thanh khoản muốn thêm thanh khoản vào bể thanh khoản, sẽ thất bại nếu nhà cung cấp không đủ lượng token muốn cung cấp:

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Phần mềm đồ họa

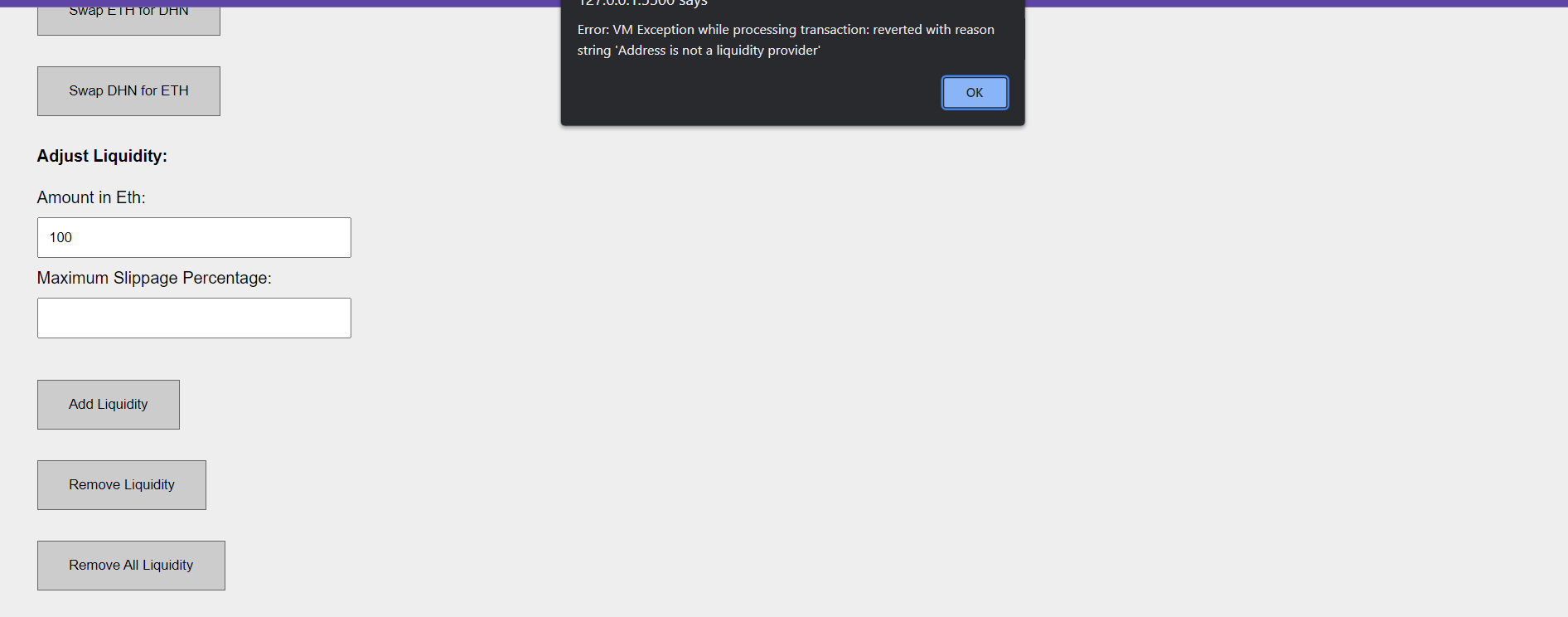
Mô tả được tạo tự động

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Biểu tượng máy tính

Mô tả được tạo tự động

### c. Khi người cung cấp muốn rút thanh khoản

Khi rút 1 phần thanh khoản sẽ thất bại khi người đó không phải là nhà cung cấp thanh khoản, rút quá số tiền mà người đó đang đóng góp và khi rút làm bể thanh khoản bằng 0:



Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Biểu tượng máy tính

Mô tả được tạo tự động

Ảnh có chứa phần mềm, ảnh chụp màn hình, văn bản, Phần mềm đa phương tiện

Mô tả được tạo tự động

### c. Khi người cung cấp muốn rút hết thanh khoản

Khi rút 1 phần thanh khoản sẽ thất bại khi người đó không phải là nhà cung cấp thanh khoản, khi rút làm bể thanh khoản bằng 0:

Ảnh có chứa văn bản, phần mềm, Phần mềm đa phương tiện, Biểu tượng máy tính

Mô tả được tạo tự động

# IV. Kết luận

Trong quá trình nghiên cứu và xây dựng hai dự án nhỏ liên quan đến phi tập trung tương tự Splitwise và Uniswap, nhóm đã có được một số kết quả quan trọng và học hỏi thêm được nhiều kiến thức mới đối với Blockchain đặc biệt trong vai trò ứng dụng đời sống.

Hệ thống tương tự Splitwise: Dự án xây dựng hệ thống phi tập trung tương tự Splitwise đã thành công trong việc triển khai chức năng ghi lại khoản nợ và tính toán nợ nần giữa các thành viên một cách dễ dàng. Hệ thống này mô phỏng giúp giảm bớt sự phức tạp và mâu thuẫn trong việc quản lý các khoản chi tiêu chung.

Hệ thống tương tự Uniswap: Dự án xây dựng phiên bản đơn giản của Uniswap cũng đạt được những kết quả. Nhóm đã triển khai chức năng trao đổi giữa ETH và một đồng token tự tạo. Người dùng có thể thực hiện swap giữa hai tài sản một cách dễ dàng và hiệu quả. Điều này mở ra cơ hội cho các người dùng tham gia vào thị trường thanh khoản phi tập trung và giao dịch các loại tài sản số. Ngoài ra còn có cơ thế thêm hoặc rút thanh khoản đối với những nhà cung cấp thanh khoản muốn thêm thanh khoản và thệ thống.

Nhìn chung phi tập trung là một lĩnh vực đầy tiềm năng. Sự phát triển của công nghệ blockchain đã mở ra cơ hội để xây dựng các ứng dụng phi tập trung, giúp loại bỏ sự tập trung quyền lực và tạo ra các hệ thống công bằng và minh bạch hơn.

Tổng kết lại, việc nghiên cứu và xây dựng hai dự án liên quan đến phi tập trung đã giúp nhóm có cái nhìn tổng quan về lĩnh vực này và những tiềm năng mà nó mang lại. Qua đó mở rộng hơn những cơ hội tìm hiểu và phát triển nền tảng công nghệ blockchain trong tương lại.

V. Tài liệu tham khảo  
[1]  Slide bài giảng “Blockchain" - Thầy Nguyễn Bình Minh, Trường Công nghệ thông tin và truyền thông, Đại học Bách Khoa Hà Nội

[2] <https://soliditylang.org/>

[3] <https://docs.ethers.org/v5/>

[4] <https://viblo.asia/p/data-structure-algorithm-graph-algorithms-breadth-first-search-bfs-gwd43kMM4X9>

[5] <https://academy.binance.com/vi/articles/what-is-uniswap-and-how-does-it-work>

[6] <https://devweb3.net/deep-dive-into-uniswap-v2-inner-workings/>