ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

PROPOSAL CHI TIẾT
MÔN BLOCKCHAIN: NỀN TẢNG, ỨNG DỤNG VÀ BẢO MẬT

Đề tài: Blockchain for Trust Rating and Fraud Detection in E-Commerce

GVHD: TS.Nguyễn Ngọc Tự

Nhóm:

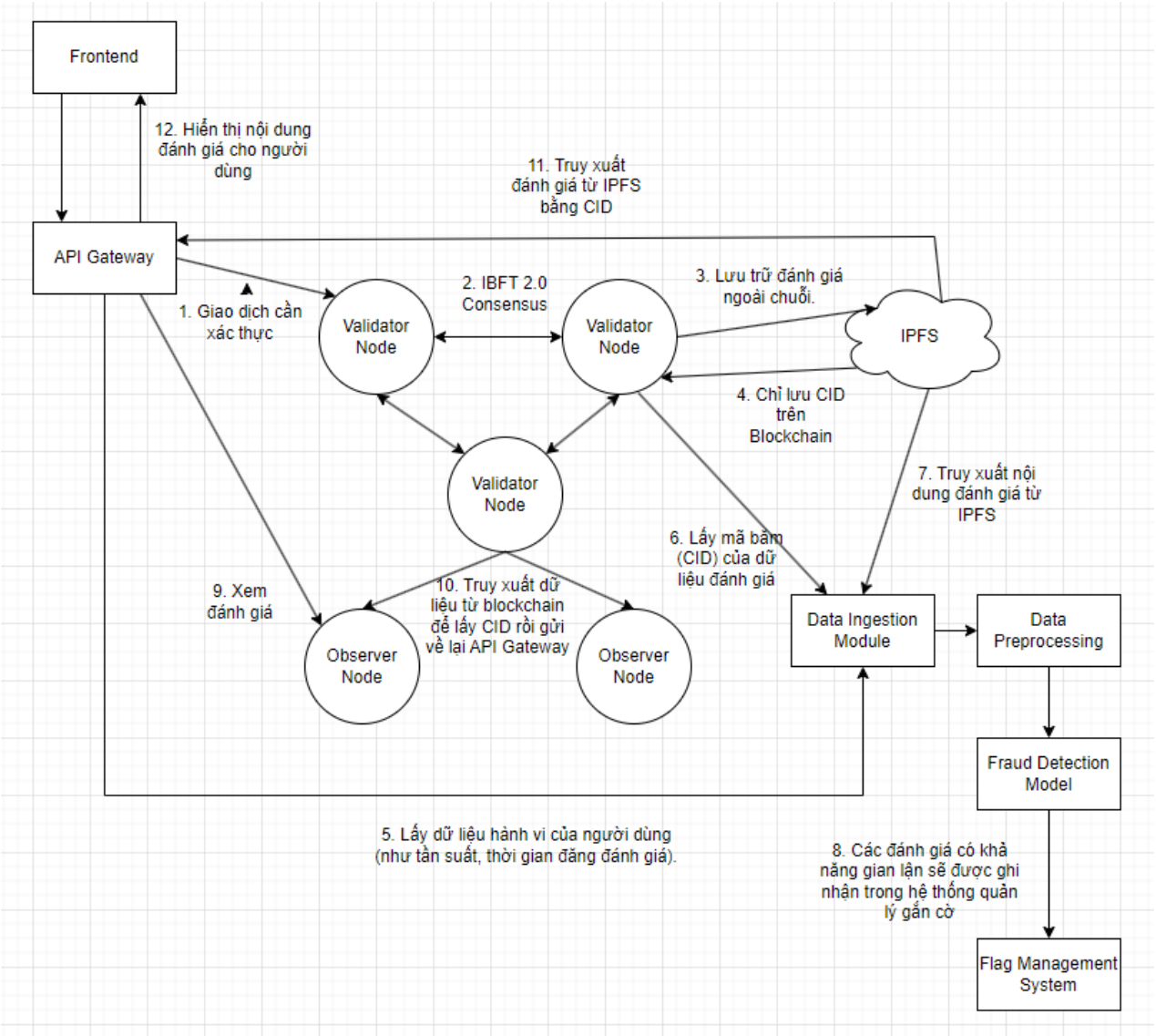
Nguyễn Đại Nghĩa	**21521182**
Phạm Hoàng Phúc	**21521295**

I. GIỚI THIỆU (INTRODUCTION)

1. **Bối cảnh:**
   Trong những năm gần đây, thương mại điện tử bùng nổ mạnh mẽ với hàng triệu giao dịch diễn ra mỗi ngày trên các sàn thương mại trực tuyến như Amazon, eBay hay Shopee. Sự tiện lợi của việc mua sắm trực tuyến đã thu hút hàng triệu người tiêu dùng, bên cạnh đó cũng đi kèm với nhiều thách thức. Một trong những vấn đề lớn nhất là việc xây dựng và duy trì niềm tin giữa người tiêu dùng và các nhà cung cấp.
2. **Thách thức:**
   Đánh giá sản phẩm và người bán đóng vai trò quan trọng trong quyết định mua sắm của người tiêu dùng, tuy nhiên các hệ thống đánh giá hiện tại đang tồn đọng các vấn đề sau:
   -Thiếu tính minh bạch, người tiêu dùng không thể biết được cách thức mà các đánh giá được thu thập và quản lý.
   -Kiểm soát tập trung khiến cho đánh giá có thể bị xóa hoặc chỉnh sửa.
   -Đánh giá giả mạo do người dùng tạo ra.
   -Khó theo dõi lịch sử đánh giá.
3. **Mục tiêu:**
   Mục tiêu của chúng em trong đồ án môn học này là xây dựng hệ thống đánh giá sản phẩm dựa trên công nghệ Blockchain nhằm loại bỏ kiểm soát tập trung, tăng cường tính minh bạch, ngăn chặn chỉnh sửa hoặc xóa đánh giá. Ngoài ra, tích hợp thêm các mô hình machine learning vào hệ thống để cải thiện khả năng phát hiện các đánh giá giả mạo.

II. KIẾN TRÚC HỆ THỐNG ĐỀ XUẤT

Dưới đây là kiến trúc của hệ thống mà nhóm dự định sẽ thực hiện:



Luồng dữ liệu khi người dùng thực hiện đánh giá: Từ 1 đến 8.
Luồng dữ liệu khi người dùng thực hiện việc xem các đánh giá: Từ 9 đến 12.

III. PHƯƠNG PHÁP TRIỂN KHAI

1. Phát Triển Hợp Đồng Thông Minh (Smart Contract Development)

1.1 Hợp đồng thông minh ghi nhận và Lưu trữ Đánh giá (Record and Store Reviews)

Chức năng: Cho phép người mua đăng đánh giá sau khi hoàn tất giao dịch mua hàng.

Quy trình:

Xác thực người mua: Hợp đồng kiểm tra ID giao dịch để đảm bảo rằng chỉ những người mua thực sự của sản phẩm mới có quyền đánh giá.

Nhận và mã hóa đánh giá: Sau khi xác nhận quyền đăng đánh giá, hợp đồng sẽ lưu trữ nội dung đánh giá dưới dạng hash (mã băm) trên blockchain.

Gắn mã định danh đánh giá: Mỗi đánh giá sẽ được gắn một mã định danh duy nhất (review ID) để đảm bảo tính duy nhất và dễ dàng truy xuất trong hệ thống.

Lợi ích: Đảm bảo mỗi đánh giá là duy nhất, không bị trùng lặp và có nguồn gốc rõ ràng.

1.2 Hợp đồng thông minh phân phối Phần thưởng cho Đánh giá Trung thực (Reward Honest Reviews)

Chức năng: Khuyến khích người dùng đăng đánh giá trung thực thông qua hệ thống phần thưởng.

Quy trình:

Xác định điều kiện phân phối phần thưởng: Hợp đồng sẽ kiểm tra đánh giá để xác định xem đánh giá có đáp ứng các tiêu chí để được nhận phần thưởng hay không (như độ trung thực, không có dấu hiệu gian lận).

Cấp phát phần thưởng: Nếu đáp ứng điều kiện, hợp đồng sẽ tự động phân phối token hoặc điểm thưởng vào tài khoản của người dùng.

Lưu trữ thông tin phần thưởng: Hợp đồng sẽ lưu lại dữ liệu về các phần thưởng đã cấp phát nhằm kiểm soát và ngăn chặn việc lạm dụng phần thưởng.

Lợi ích: Tăng tính tích cực của người dùng và đảm bảo các đánh giá nhận được là có giá trị thực sự.

1.3 Hợp đồng thông minh xác thực và Gắn cờ các Đánh giá Đáng ngờ (Verify and Flag Suspicious Reviews)

Chức năng: Tự động kiểm tra và gắn cờ các đánh giá có dấu hiệu gian lận.

Quy trình:

Phân tích đánh giá bằng AI/ML: Trước khi lưu trữ đánh giá, hệ thống AI/ML sẽ phân tích nội dung và các yếu tố của đánh giá (ví dụ: cụm từ, thời gian, địa chỉ IP).

Gắn cờ đánh giá: Nếu AI phát hiện dấu hiệu gian lận, hợp đồng sẽ gắn trạng thái "cảnh báo" (flagged) cho đánh giá, yêu cầu quản trị viên xác nhận.

Lưu trữ trạng thái đánh giá: Đánh giá bị gắn cờ sẽ được lưu trữ với trạng thái đặc biệt, không hiển thị công khai cho đến khi quản trị viên xác nhận.

Lợi ích: Giúp phát hiện và ngăn chặn các đánh giá giả mạo hoặc đáng ngờ trước khi công khai.

1.4 Hợp đồng thông minh quản lý Quyền truy cập và Phân quyền (Access and Permission Management)

Chức năng: Đảm bảo rằng chỉ những người dùng hợp lệ mới có quyền ghi nhận đánh giá và truy cập thông tin.

Quy trình:

Xác thực vai trò: Trước khi thực hiện các hành động như ghi nhận đánh giá hoặc gắn cờ, hợp đồng sẽ xác thực vai trò của người dùng (người mua, người bán, quản trị viên).

Phân quyền theo vai trò: Hợp đồng chỉ cho phép những người dùng có quyền thực hiện các chức năng tương ứng (ví dụ: quản trị viên mới có quyền xử lý đánh giá bị gắn cờ).

Lợi ích: Bảo vệ hệ thống khỏi các hành vi xâm nhập trái phép và bảo vệ quyền riêng tư của người dùng.

1.5 Phát triển và Kiểm thử Hợp đồng Thông minh (Smart Contract Coding and Testing)

Viết mã hợp đồng thông minh: Sử dụng Chaincode với Hyperledger Fabric hoặc solidity với Hyperledger Besu để viết mã cho các chức năng đã xác định.

Kiểm thử hợp đồng thông minh: Sử dụng các công cụ tích hợp của Hyperledger để kiểm thử các chức năng của hợp đồng.

Kiểm thử bảo mật: Sử dụng các công cụ như MythX và Slither để tìm kiếm các lỗ hổng bảo mật phổ biến (re-entrancy, integer overflow) và vá các lỗ hổng này trước khi triển khai.

1.6 Triển khai trên Mạng (Deploying on Network)

Triển khai thử nghiệm: Đưa hợp đồng lên mạng thử nghiệm để đánh giá hiệu quả và tính ổn định của hệ thống.

Triển khai trên mạng chính thức: Sau khi hoàn tất các thử nghiệm và điều chỉnh cần thiết, hợp đồng sẽ được triển khai trên mạng chính thức.

2. Tích Hợp AI/ML cho Phát Hiện Gian Lận (AI/ML Integration for Fraud Detection)

Bởi vì đây là đồ án chuyên về blockchain nên nhóm em sẽ không đi quá sâu vào mô hình mãy học mà thay vào đó sẽ cố gắng tìm được một mô hình học máy đã được train cho việc này, còn nếu không tìm được thì có thể nhóm em sẽ thực hiện các bước như sau:

2.1 Mô hình Phát hiện Gian lận (Fraud Detection Model)

Thuật toán Machine Learning: Sử dụng các thuật toán học máy (ML) như Random Forest, SVM (Support Vector Machine) hay Naive Bayes để phân loại các đánh giá là trung thực hay gian lận.

2.2 Phân tích Hành vi Người dùng (User Behavior Analysis)

Dữ liệu hành vi người dùng: Bao gồm thời gian đánh giá, số lượng đánh giá liên tục, các cụm từ được sử dụng, tần suất đánh giá và địa chỉ IP.

Hệ thống gắn cờ (Flagging System): Dựa trên phân tích hành vi, hệ thống có thể gắn cờ các đánh giá có tính chất bất thường, ví dụ: một người dùng đăng nhiều đánh giá trong thời gian ngắn hoặc từ cùng một địa chỉ IP.

2.3 Thu thập và Xử lý Dữ liệu (Data Collection and Preprocessing)

Thu thập dữ liệu: Thu thập các đánh giá từ nền tảng thương mại điện tử và các thông tin hành vi liên quan. Các dữ liệu bao gồm:

Nội dung đánh giá (text data)

Dữ liệu về người dùng: thời gian đăng, địa chỉ IP, tần suất đánh giá.

Xử lý dữ liệu:

Xử lý ngôn ngữ tự nhiên (NLP): Làm sạch văn bản đánh giá, loại bỏ các từ không cần thiết và thực hiện các kỹ thuật như stemming hoặc lemmatization để chuẩn hóa dữ liệu.

Mã hóa dữ liệu: Dữ liệu văn bản sẽ được chuyển đổi thành các vector từ (word vectors) bằng cách sử dụng TF-IDF (Term Frequency-Inverse Document Frequency), Word2Vec hoặc BERT để đưa vào mô hình ML.

2.4 Tích hợp Hệ thống Phát hiện Gian lận vào Hợp đồng Thông minh (Integration with Smart Contracts)

Kết nối hệ thống AI với hợp đồng thông minh: Khi một đánh giá mới được tạo ra, hệ thống sẽ tự động gửi dữ liệu tới mô hình AI để phân tích. Nếu phát hiện gian lận, hệ thống sẽ gắn cờ (flag) và lưu trạng thái này vào hợp đồng thông minh.

Gắn cờ đánh giá: Hợp đồng thông minh sẽ đánh dấu các đánh giá bị gắn cờ và yêu cầu quản trị viên xác minh trước khi cho phép công khai.

2.5 Kỹ thuật Phát hiện Gian lận Dựa trên Hành vi (Behavioral Fraud Detection Techniques)

a. Phân tích thời gian (Temporal Analysis)

Phân tích chuỗi thời gian: Phân tích các mẫu thời gian của các đánh giá từ một người dùng, phát hiện các chuỗi đánh giá đăng trong thời gian ngắn bất thường.

Tần suất và thời gian đánh giá: Nếu một người dùng đăng quá nhiều đánh giá trong một khoảng thời gian ngắn hoặc trong một khung giờ nhất định, đó có thể là dấu hiệu gian lận.

b. Phân tích ngữ nghĩa và nội dung (Semantic and Content Analysis)

Phân tích ngữ nghĩa: Sử dụng các mô hình NLP để phân tích nội dung đánh giá, phát hiện các cụm từ hoặc ngữ cảnh giống nhau giữa các đánh giá.

Phân tích cấu trúc và từ vựng: Kiểm tra xem có các cụm từ hoặc cấu trúc giống nhau trong nhiều đánh giá khác nhau hay không. Đánh giá giả mạo thường có cấu trúc hoặc từ ngữ lặp lại.

c. Phân tích địa chỉ IP và thiết bị (IP Address and Device Analysis)

Theo dõi địa chỉ IP: Phát hiện các đánh giá từ cùng một địa chỉ IP hoặc từ cùng một khu vực địa lý, dấu hiệu cho thấy có thể một người dùng đang tạo ra nhiều tài khoản để đánh giá giả.

Phân tích thiết bị: Nếu một số lượng lớn các đánh giá đến từ cùng một thiết bị hoặc thông tin trình duyệt, hệ thống có thể gắn cờ đánh giá này.

3. Lưu Trữ Dữ Liệu Ngoài Chuỗi (Off-chain Data Storage)

Hệ thống thương mại điện tử thường yêu cầu lưu trữ lượng lớn dữ liệu đánh giá và các thông tin liên quan. Nếu lưu trữ trực tiếp trên blockchain, các vấn đề sau có thể phát sinh:

- Tốn kém chi phí: Phí giao dịch blockchain tăng theo dung lượng dữ liệu lưu trữ, dẫn đến chi phí cao nếu lưu toàn bộ dữ liệu đánh giá.

- Giới hạn kích thước: Blockchain có giới hạn về kích thước của mỗi giao dịch, không phù hợp để lưu trữ lượng lớn nội dung đánh giá.
- Giảm hiệu suất: Lưu dữ liệu lớn trực tiếp trên blockchain làm tăng khối lượng xử lý, gây chậm trễ và ảnh hưởng đến hiệu suất mạng.

Giải pháp là lưu trữ dữ liệu ngoài chuỗi (off-chain) trên hệ thống lưu trữ phân tán như IPFS (InterPlanetary File System) và chỉ lưu CID (Content Identifier) của dữ liệu trên blockchain. CID là mã định danh duy nhất của dữ liệu trên IPFS, có thể dùng để truy xuất và xác thực dữ liệu mà không cần lưu nội dung thực trên blockchain.

3.1 Lựa chọn Hệ thống Lưu trữ Ngoài Chuỗi (Off-chain Storage Options)

IPFS (InterPlanetary File System):

Hệ thống lưu trữ phi tập trung, cung cấp mã định danh duy nhất (CID) cho mỗi nội dung. CID này dựa trên nội dung của dữ liệu, giúp đảm bảo rằng nếu dữ liệu bị thay đổi, CID cũng thay đổi.

3.2 Quy Trình Lưu trữ Ngoài Chuỗi (Off-chain Storage Workflow)

a. Quy trình Lưu trữ Đánh giá trên IPFS

Bước 1: Chuẩn bị dữ liệu:

Nội dung đánh giá, ID người dùng, ID sản phẩm và thời gian đăng đánh giá được chuẩn hóa thành một định dạng cụ thể.

Dữ liệu được xử lý sơ bộ để đảm bảo tính nhất quán trước khi lưu trữ.

Bước 2: Lưu trữ đánh giá trên IPFS:

Dữ liệu đánh giá hoàn chỉnh được tải lên IPFS. IPFS sẽ lưu trữ dữ liệu và trả về một CID (Content Identifier), đại diện duy nhất cho nội dung của dữ liệu này.

CID này là "địa chỉ" duy nhất của dữ liệu đánh giá trên mạng IPFS.

Bước 3: Lưu CID trên blockchain:

CID của dữ liệu đánh giá sẽ được lưu trên blockchain cùng với một số thông tin cần thiết khác nếu cần, như ID người dùng, ID sản phẩm, và thời gian đăng.

CID là tất cả những gì cần lưu trên blockchain để xác thực tính toàn vẹn của đánh giá. Khi cần, CID có thể dùng để truy xuất nội dung đánh giá trên IPFS.

b. Truy xuất và Xác minh Dữ liệu từ IPFS

Truy xuất dữ liệu đánh giá từ IPFS:

Khi người dùng muốn xem đánh giá, hệ thống sẽ truy xuất CID từ blockchain, sau đó dùng CID để tìm và lấy dữ liệu từ IPFS.

Do IPFS là mạng lưu trữ phi tập trung, việc truy xuất nhanh và đảm bảo dữ liệu không bị thay đổi sau khi đăng.

Xác minh tính toàn vẹn của dữ liệu:

CID dựa trên nội dung của đánh giá, nên nếu nội dung đánh giá bị chỉnh sửa, CID sẽ không còn khớp với CID lưu trên blockchain.
Điều này giúp hệ thống phát hiện bất kỳ sự thay đổi nào, đảm bảo rằng dữ liệu đánh giá không bị chỉnh sửa sau khi lưu trữ.

3.3 Kết nối giữa IPFS và Blockchain

Smart Contract: Hợp đồng thông minh sẽ đóng vai trò lưu trữ mã băm của dữ liệu IPFS, tạo ra kết nối giữa blockchain và IPFS để xác thực tính toàn vẹn của dữ liệu.
Các API kết nối: Sử dụng các API của IPFS để tải lên và truy xuất dữ liệu, đồng thời kết nối API này với blockchain để có thể xác thực mã băm một cách tự động.

3.4 Đảm bảo tính sẵn sàng của dữ liệu (Data Availability)

Nhiều bản sao trên IPFS: IPFS tự động sao chép dữ liệu trên nhiều node trong mạng, đảm bảo rằng dữ liệu luôn sẵn sàng ngay cả khi một số node gặp sự cố.
Kế hoạch sao lưu và khôi phục: Thiết lập các bản sao lưu định kỳ cho dữ liệu quan trọng, đồng thời có kế hoạch khôi phục để tránh mất mát dữ liệu nếu có sự cố.

4. Thiết Lập Mạng Blockchain Consortium (Consortium Blockchain Setup)

Lý do lựa chọn mạng blockchain dạng Consortium Blockchain vì:

- Cho phép quản lý quyền truy cập: Chỉ các bên được cấp quyền mới có thể tham gia vào mạng và thực hiện giao dịch.
- Đảm bảo quyền riêng tư: Các thành viên trong consortium có thể thiết lập các quyền riêng tư và chia sẻ dữ liệu cần thiết mà không bị công khai cho tất cả mọi người như các mạng công khai.
- Tối ưu hóa hiệu suất: Consortium blockchain có thể tùy chỉnh để xử lý khối lượng giao dịch lớn và nhanh chóng mà không cần xác minh toàn mạng như mạng công khai.

4.1 Nền tảng Blockchain

Nhóm em hiện tại đang phân vân giữa Hyperledger Fabric và Hyperledger Besu để deploy, nhưng với sự đơn giản hơn của Besu nên nhóm sẽ thực hiện trước với Besu để xem sao ạ

4.2 Thành phần chính trong Mạng Blockchain Consortium với Besu

Node (Nút mạng):

Các node đại diện cho từng thành viên tham gia trong mạng (có thể là các nhà cung cấp dịch vụ, quản trị viên nền tảng, các đối tác bán lẻ hoặc cửa hàng đối tác hoặc các bên liên quan khác nếu cần như đối tác phân phối, cơ quan giám sát độc lập,…).

Mỗi node sẽ chạy Hyperledger Besu và tham gia xác nhận, xử lý giao dịch trên mạng blockchain.

Cơ chế Đồng thuận:

Nhóm em chọn IBFT 2.0 là cơ chế đồng thuận vì:

Chịu lỗi Byzantine (Byzantine Fault Tolerant): Đảm bảo mạng vẫn hoạt động ngay cả khi một số node xác thực (validator node) gặp sự cố hoặc có hành vi không trung thực.

Khả năng đồng thuận phi tập trung: Không yêu cầu node cụ thể là validator cố định, mà cho phép tất cả các validator thay phiên nhau tham gia vào quá trình xác thực.

Tính bảo mật cao và tin cậy: Nhờ vào cơ chế bỏ phiếu và xác thực của IBFT 2.0, hệ thống bảo đảm an toàn và tin cậy ngay cả khi có sự cố hoặc tấn công.

Quản lý Quyền và Danh tính:

Mạng permissioned yêu cầu quản lý danh tính cho từng node tham gia để đảm bảo chỉ các thành viên đã được xác thực mới có thể tham gia vào mạng.

Mỗi node sẽ cần có một chứng chỉ (Certificate) hoặc khoá công khai (Public Key), quản lý thông qua một cơ quan chứng thực (Certificate Authority).

4.3 Thiết Lập Mạng Blockchain Consortium với IBFT 2.0

Bước 1: Chuẩn bị các Node và Hệ thống Môi trường

a. Thiết lập hạ tầng:

Đảm bảo rằng mỗi thành viên consortium sẽ có ít nhất một node tham gia mạng. Mỗi node phải được cài đặt Hyperledger Besu.

Các node này sẽ hoạt động dưới dạng validator nodes để tham gia vào cơ chế đồng thuận IBFT 2.0.

b. Cài đặt Hyperledger Besu

Bước 2: Cấu hình Genesis File cho IBFT 2.0

Tạo Genesis File

Cấu hình chi tiết cho Genesis File

Bước 3: Khởi động và Kết nối các Node với Genesis File

Thiết lập khóa cho mỗi node

Khởi động node với Genesis File

Kết nối các node với nhau

Bước 4: Cấu hình và Quản lý Quyền Truy cập (Permissioning)

Danh sách Permissioning

Xác thực danh tính cho mỗi node

Cơ chế bỏ phiếu quản trị

Bước 5: Triển khai và Quản lý Hợp đồng Thông minh

Bước 6: Giám sát và Quản lý Mạng Consortium với IBFT 2.0

Công cụ giám sát:

Sử dụng Hyperledger Explorer hoặc các công cụ như Prometheus và Grafana để theo dõi tình trạng mạng, các giao dịch và khối mới tạo ra.

Giám sát các validator node để phát hiện các vấn đề kịp thời và đảm bảo mạng hoạt động ổn định.

4.4 Kiểm thử và Khởi động Mạng

Kiểm thử đồng thuận IBFT 2.0:

Chạy thử các giao dịch để đảm bảo rằng các node có thể đồng thuận thành công và mỗi giao dịch được ghi vào blockchain như mong đợi.

Kiểm thử khả năng chịu lỗi bằng cách tạm dừng hoặc làm gián đoạn một số node và quan sát khả năng duy trì đồng thuận của hệ thống.

Chính thức khởi động mạng:

Sau khi hoàn tất kiểm thử, chính thức triển khai mạng cho hệ thống đánh giá và phát hiện gian lận trong rating.

5. Thiết lập nơi tương tác giữa người dùng và hệ thống

5.1 Frontend

Chức năng chính:

Đăng nhập và Xác thực: Người dùng đăng nhập vào hệ thống để thực hiện các thao tác đánh giá. Frontend có thể hiển thị giao diện đăng nhập và gửi thông tin xác thực đến API Gateway để đảm bảo rằng người dùng đã hoàn tất giao dịch trước khi đánh giá.

Đăng đánh giá: Sau khi người dùng mua sản phẩm, giao diện sẽ có chức năng cho phép người mua đăng đánh giá.

Xem đánh giá và truy xuất dữ liệu: Người mua và người bán có thể xem các đánh giá đã được lưu trên hệ thống.

Quy trình thao tác của người dùng:

Đăng nhập: Người dùng truy cập ứng dụng và đăng nhập. Frontend gửi thông tin xác thực tới API Gateway.

Đăng đánh giá: Sau khi đăng nhập, người mua có thể chọn sản phẩm đã mua và gửi đánh giá. Đánh giá này sẽ được chuyển tới API Gateway.

Xem đánh giá: Người dùng chọn sản phẩm và yêu cầu truy xuất đánh giá từ blockchain.

5.2 API Gateway

Chức năng chính:

Xác thực yêu cầu của người dùng: API Gateway nhận các yêu cầu từ frontend và xác thực quyền truy cập trước khi chuyển tiếp các yêu cầu đến blockchain. Ví dụ, chỉ người mua đã hoàn tất giao dịch mới được đăng đánh giá.

Điều phối luồng dữ liệu: API Gateway xử lý các yêu cầu từ người dùng và gửi đến các node trong Blockchain Layer như validator hoặc observer node để thực hiện các thao tác lưu trữ hoặc truy xuất dữ liệu.

Phản hồi yêu cầu của người dùng: Sau khi xử lý xong yêu cầu, API Gateway sẽ nhận kết quả từ blockchain và trả lại cho frontend để hiển thị cho người dùng.

Quy trình xử lý trong API Gateway:

Xác thực người dùng: Khi người dùng gửi yêu cầu đăng đánh giá, API Gateway xác thực quyền của người dùng dựa trên thông tin đăng nhập. Nếu người dùng hợp lệ và đã mua sản phẩm, yêu cầu sẽ được chấp nhận.

Chuyển tiếp yêu cầu tới Blockchain Layer:
Nếu người dùng gửi đánh giá mới, API Gateway sẽ chuyển yêu cầu đến validator nodes trong Blockchain Layer để xác thực và ghi nhận.

Nếu người dùng yêu cầu xem đánh giá, API Gateway sẽ chuyển yêu cầu đến observer nodes hoặc truy xuất CID để lấy dữ liệu từ IPFS.

Trả lại kết quả cho Frontend: Sau khi blockchain xử lý yêu cầu xong, API Gateway sẽ nhận kết quả và gửi lại cho frontend để hiển thị cho người dùng.

IV. CÔNG CỤ VÀ CÔNG NGHỆ SỬ DỤNG

Nền tảng Blockchain:

Hyperledger Besu

Cơ chế Đồng thuận:

IBFT 2.0

Phát triển Hợp đồng Thông minh:

Solidity,

Truffle Suite (Bộ công cụ phát triển hợp đồng thông minh gồm Truffle (framework), Ganache (mạng blockchain cá nhân), và Drizzle (thư viện frontend). Hỗ trợ quá trình phát triển, kiểm thử và triển khai hợp đồng thông minh dễ dàng hơn).

Giám sát và Quản lý Mạng:

Hyperledger Explorer

Lưu trữ Dữ liệu Ngoài Chuỗi:

IPFS

V. KẾT LUẬN

VI. TÀI LIỆU THAM KHẢO