TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ**

**BLOCKCHAIN VÀ**

**CÔNG NGHỆ SỔ CÁI PHÂN TÁN**

**HỆ THỐNG ĐẤU GIÁ**

**TRỰC TUYẾN PHI TẬP TRUNG**

**LÊ KHẮC THANH TÙNG - 52100943**

**TRẦN VĂN HẢI - 52100958**

**NGUYỄN TRỌNG PHÚC - 52100990**

**VÕ NGUYÊN PHÚ QUÍ - 52100996**

**TRẦN HỮU TÀI - 52100997**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ**

**BLOCKCHAIN VÀ**

**CÔNG NGHỆ SỔ CÁI PHÂN TÁN**

**HỆ THỐNG ĐẤU GIÁ**

**TRỰC TUYẾN PHI TẬP TRUNG**

**LÊ KHẮC THANH TÙNG - 52100943**

**TRẦN VĂN HẢI - 52100958**

**NGUYỄN TRỌNG PHÚC - 52100990**

**VÕ NGUYÊN PHÚ QUÍ - 52100996**

**TRẦN HỮU TÀI - 52100997**

Người hướng dẫn

**ThS. Phạm Thái Kỳ Trung**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

**LỜI CẢM ƠN**

Để hoàn thành bài báo cáo này, chúng em xin gửi lời cảm ơn chân thành đến Ban giám hiệu trường Đại Học Tôn Đức Thắng vì đã tạo điều kiện thuận lợi nhất cho sinh viên khi học tập.

Chúng em xin chân thành cảm ơn giảng viên bộ môn - ThS. Phạm Thái Kỳ Trung đã tận tình giảng dạy chi tiết, đầy đủ kiến thức để chúng em vận dụng vào bài báo cáo này.

Do chưa có nhiều kinh nghiệm trong việc làm báo cáo và sự hạn chế về kiến thức nên bài báo cáo không tránh khỏi những thiếu sót. Rất mong nhận được những ý kiến, đóng góp và phê bình từ phía cô để bài báo cáo được hoàn thiện hơn.

Lời cuối cùng, chúng em xin kính chúc cô sức khỏe, thành công trong cuộc sống.

*TP. Hồ Chí Minh, ngày 30 tháng 12 năm 2023*

*Tác giả*

*(Ký tên và ghi rõ họ tên)*

*Lê Khắc Thanh Tùng*

*Trần Văn Hải*

*Nguyễn Trọng Phúc*

*Võ Nguyên Phú Quí*

*Trần Hữu Tài*

**CÔNG TRÌNH ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi và được sự hướng dẫn khoa học của ThS. Phạm Thái Kỳ Trung. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung Dự án của mình**. Trường Đại học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày 30 tháng 12 năm 2023*

*Tác giả*

*(Ký tên và ghi rõ họ tên)*

*Lê Khắc Thanh Tùng*

*Trần Văn Hải*

*Nguyễn Trọng Phúc*

*Võ Nguyên Phú Quí*

*Trần Hữu Tài*

**MỤC LỤC**

[DANH MỤC HÌNH VẼ 5](#_Toc1292474737)

[CHƯƠNG 1. MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI 1](#_Toc168684548)

[1.1 Đặt vấn đề 1](#_Toc1404077006)

[1.2 Mục tiêu thực hiện đề tài 1](#_Toc1972357406)

[CHƯƠNG 2. CƠ SỞ LÝ THUYẾT 2](#_Toc366121081)

[2.1 Blockchain 2](#_Toc1772809227)

[2.1.1 Định nghĩa 2](#_Toc1699127961)

[*2.1.2* Cơ chế hoạt động 3](#_Toc1933108228)

[*2.1.3* Lợi ích và hạn chế 5](#_Toc1607188695)

[2.2 Smart Contract 6](#_Toc2011762041)

[*2.2.1* Định nghĩa 6](#_Toc1394981624)

[*2.2.2* Cơ chế hoạt động 6](#_Toc711509583)

[*2.2.3* Lợi ích của smart contract 7](#_Toc1515381338)

[2.3 Một số nền tảng phổ biến 9](#_Toc136173356)

[2.3.1 NEAR Protocol 10](#_Toc427459945)

[2.3.2 ReactJS 10](#_Toc377435414)

[2.3.3 NodeJS 11](#_Toc2005168134)

[2.3.4 MongoDB 12](#_Toc429768686)

[CHƯƠNG 3. PHÂN TÍCH VÀ THIẾT KẾ 13](#_Toc1566536470)

[3.1 Sơ đồ Use case tổng quát 13](#_Toc2081383798)

[3.2 Tổng quan về mô hình ứng dụng công nghệ blockchain vào hệ thống 14](#_Toc1799604001)

[3.3 Xây dựng smart contract 14](#_Toc1344866527)

[CHƯƠNG 4. THỰC NGHIỆM 21](#_Toc744673444)

[4.1 Cài đặt thực nghiệm 21](#_Toc1263752330)

[4.1.1 Localnet 27](#_Toc1743698691)

[*4.1.2* Testnet 29](#_Toc746546544)

[4.2 Kết quả thực nghiệm 30](#_Toc1636289741)

[CHƯƠNG 5. KẾT LUẬN 37](#_Toc1818975178)

[5.1 Kết luận 37](#_Toc724120971)

[5.2 Hướng phát triển 37](#_Toc1380410126)

[TÀI LIỆU THAM KHẢO 39](#_Toc1987659726)

# DANH MỤC HÌNH VẼ

[Hình 1 Sơ đồ use case tổng quát 17](#_Toc199970092)

[Hình 2 Mô hình ứng dụng 18](#_Toc1194371533)

[Hình 3 Cấu trúc smart contract 18](#_Toc1369550613)

[Hình 4 Khởi tạo smart contract trong file lib.rs 20](#_Toc1613130894)

[Hình 5 Tạo các struct 20](#_Toc585863526)

[Hình 6 Hiện thực các phương thức đã khai báo 21](#_Toc42369896)

[Hình 7 Tạo cuộc đấu giá 21](#_Toc1417425069)

[Hình 8 Phương thức để người dùng tham gia vào một cuộc đấu giá 22](#_Toc1338468864)

[Hình 9 Phương thức cho người dùng tham gia cuộc đấu giá 23](#_Toc1426801985)

[Hình 10 Kết thúc cuộc đấu giá 24](#_Toc611629473)

[Hình 11 Trả lại số tiền tương ứng cho những người không thắng 24](#_Toc1505918426)

[Hình 12 Chuyển số tiền cho người bán 24](#_Toc980319397)

[Hình 13 Trang chủ của website 34](#_Toc286358380)

[Hình 14 Liên kết ví 35](#_Toc179563333)

[Hình 15 Trang thông tin 35](#_Toc354704534)

[Hình 16 Giao diện chính 36](#_Toc1367526573)

[Hình 17 Giao diện tạo sản phẩm 36](#_Toc1098677939)

[Hình 18 Giao diện tạo cuộc đấu giá 37](#_Toc1334750713)

[Hình 19 Giao diện mời người khác tham gia tổ chức 37](#_Toc1870201424)

[Hình 20 Giao diện xem các cuộc đấu giá đang diễn ra 38](#_Toc1564108813)

[Hình 21 Giao diện đấu giá 38](#_Toc1135349435)

[Hình 22 Danh sách người tham gia đấu giá 39](#_Toc1056803656)

[Hình 23 Thông tin giao dịch 39](#_Toc815616898)

[Hình 24 Mã QR 40](#_Toc92888181)

# MỞ ĐẦU VÀ TỔNG QUAN ĐỀ TÀI

## Đặt vấn đề

Hình thức đấu giá truyền thống thường tổ chức trực tiếp, tạo nên sự cản trở về khoảng cách. Một số hệ thống đấu giá trực tuyến hiện nay cũng đã xuất hiện, nhưng vẫn gặp những hạn chế về sự tin tưởng, phụ thuộc nhiều vào bên thứ 3 như bên thanh toán, vận chuyển. Điều này tạo nên những lo ngại từ phía người dùng đối với hệ thống. Và một công nghệ đã được ra đời để giải quyết những vấn đề trên, thay đổi cách các ứng dụng tương tác với dữ liệu, đó là blockchain.

Tận dụng những ưu điểm của blockchain để tạo ra một hệ thống đấu giá trực tuyến an toàn và tin cậy. Một trong những tính chất cơ bản của blockchain đó chính là tính minh bạch, điều này giúp người dùng dễ dàng truy xuất nguồn gốc của những sản phẩm, theo dõi quá trình đấu giá và các giao dịch. Ngoài ra, blockchain còn là một công nghệ mà không cần đến sự can thiệp của bên thứ 3 về tài chính (các ngân hàng), tạo nên sự tin tưởng trong các giao dịch trong cuộc đấu giá. Blockchain còn đảm bảo được tính riêng tư của người dùng, tất cả giao dịch được thực hiện qua địa chỉ ví.

## 

## Mục tiêu thực hiện đề tài

Mục tiêu của đề tài là ứng dụng blockchain vào thực tế. Áp dụng những thế mạnh của blockchain để tạo ra một nền tảng với độ tin cậy cao. Đưa ra những ứng dụng khác của blockchain để mọi người có thể thấy được blockchain có nhiều ứng dụng chứ không chỉ về tiền tệ và giao dịch. Ngoài ra, đề tài còn có thể giúp mọi người có thể hiểu thêm về blockchain và dễ dàng tiếp cận nền tảng công nghệ này.

# CƠ SỞ LÝ THUYẾT

## Blockchain

### Định nghĩa

Chuỗi khối Blockchain là một loại cơ sở dữ liệu, thông tin được lưu trữ trong các khối và liên kết với nhau. Hiểu theo ngữ nghĩa của từng từ thì Block nghĩa là “khối”, chain nghĩa là “chuỗi”. Thông tin trong khối, các liên kết sẽ được mã hóa đồng thời có thể mở rộng theo thời gian. Mỗi khi một thông tin hoặc giao dịch mới xảy ra, thông tin cũ sẽ không bị mất đi mà thay vào đó, thông tin mới sẽ được lưu vào một khối mới và lần lượt được nối vào khối cũ để tạo thành một chuỗi mới. Có thể ví chuỗi khối Blockchain như một cuốn sổ cái ghi lại toàn bộ dữ liệu trong hệ thống. Blockchain khác với các dữ liệu thông thường ở cấu trúc lưu trữ dữ liệu. Blockchain sẽ thu thập thông tin dữ liệu và nhóm chúng thành các khối chứa tập hợp nhiều thông tin.

Trải qua nhiều giai đoạn phát triển, tới thời điểm hiện tại, Blockchain đã có 04 phiên bản khác nhau, bao gồm:

* Blockchain 1.0: Dùng cho các thuật toán về tiền tệ (ví blockchain)

Công nghệ này hỗ trợ mọi giao dịch liên quan đến chuyển đổi tiền tệ, kiều hối và tạo lập hệ thống thanh toán kỹ thuật số trong phạm vi tiền điện tử bằng cách sử dụng các thuật toán về tiền tệ.

* Blockchain 2.0: Dùng trong ngành tài chính và ngân hàng

Công nghệ này được ứng dụng và xử lý các tài sản của ngành Tài chính – Ngân hàng. Các tài sản bao gồm cổ phiếu, chi phiếu, nợ, quyền sở hữu và bất kỳ điều gì có liên quan đến thỏa thuận hay hợp đồng một cách minh bạch, rõ ràng nhất.

* Blockchain 3.0: Kế thừa ưu điểm của tất cả phiên bản Blockchain trước đó đồng thời có thể tích hợp được trong nhiều ngành nghề

Công nghệ Blockchain được mở rộng và hội nhập vào đa lĩnh vực trong đời sống như y tế, giáo dục, chính phủ hay nghệ thuật.

* Blockchain 4.0: Doanh nghiệp và ứng dụng giao dịch

### Cơ chế hoạt động

Phần lớn Blockchain phần thành 4 cấp hoạt động:

**Nguyên lý mã hóa**

Blockchain được duy trì dựa trên hệ thống hàng ngang có mối liên kết chặt chẽ với nhau. Vì thế nó sẽ tạo ra một điểm khác biệt:

* Có thể xem được toàn bộ các giao dịch, trao đổi của người dùng.
* Giao dịch không cần có sự can thiệp của bên thứ 3 xử lý.
* Công nghệ lưỡi khối được mã hóa qua các hàm toán học đặc biệt.

Ngoài ra để thực hiện giao dịch trên Blockchain càn có sự trao đổi thông qua ví điện tử. Tất cả sẽ được bảo mật bằng các phương pháp mã hóa đặc biệt nhờ khóa riêng tư và khóa công khai.

Có nghĩa là khi bạn mã hóa bằng khóa Public thì chủ sở hữu Private mới là người giải mã được các nội dung và dữ liệu gửi đến. Còn khi sử dụng mã riêng tư thì bạn cần tạo nên một ký tự đặc biệt như chữ ký điện tử. Từ đó các mạng Blockchain mới có thể kiểm soát và tiến hành kiểm tra chủ thể để xác định giao dịch.

**Quy tắc cuốn sổ cái**

Mỗi nút trên hệ thống mạng lưới đều lưu trữ một bản sao của cuốn sổ kế toán. Vì vậy thông qua các nút bạn sẽ nắm được số dư tài khoản của mình. Cách thức hoạt động của Blockchain là chỉ lưu trữ lại các giao dịch mà không hề can thiệp theo dõi số dư là bao nhiêu.

Bên cạnh đó nếu muốn biết số dư trên ví điện tử của mình, người dùng phải xác nhận và kiểm tra lại các giao dịch xoay quanh ví điện tử dựa trên liên kết giao dịch trước đó. Dựa vào đó các nút liên kết sẽ xác minh chi tiết số tiền trong khi giao dịch của người dùng đó.

Tuy nhiên với cách thức hoạt động của Blockchain, bạn cần lưu ý bảo vệ mật khẩu và khóa riêng tư thật sự an toàn. Bởi khi đã đánh mất “chìa khóa” sẽ không có một đơn vị nào có thể giúp người dùng phục hồi hay lấy lại mật khẩu ví điện tử.

**Nguyên lý tạo khối**

Sau khi phát sinh giao dịch trên mạng lưới Blockchain, nhờ vào cách thức hoạt động của Blockchain, chúng sẽ được gom vào một nhóm các khối trong cùng 1 block vào 1 thời điểm đồng nhất. Mỗi một nút sẽ trở thành một khối và báo về hệ thống như một hàm ý để tạo các khối liên kết tiếp theo. Khi được cập nhật vào Blockchain, mỗi khối sẽ tích hợp lại 1 đoạn mật mã cho một hàm toán phức tạp. Để giải được bài toán này, bạn sẽ phải lựa chọn xác suất giữa các con số ngẫu nhiên.

Quy trình trong hệ thống mà 1 chuỗi sẽ được tạo ra trong khoảng thời gian là 10 phút. Nút nào giải được bài toán sẽ gắn tiếp quyền với khối tiếp theo vào chuỗi và được gửi đến toàn bộ mạng lưới.

Với cách thức hoạt động của Blockchain như thế này sẽ có ít khả năng các khối được xây dựng cùng nhau. Vì vậy sẽ không thể xuất hiện trường hợp các khối đồng loạt giải quyết 1 lúc và tạo ra các khối nối đuôi khác nhau. Do đó người dùng hoàn toàn yên tâm bởi sự đồng thuận giữa toàn bộ chuỗi các khối.

### Lợi ích và hạn chế

Với sự phức tạp của blockchain, một hình thức lưu trữ hồ sơ phi tập trung, tiềm năng của nó là gần như không có giới hạn. Từ quyền riêng tư của người dùng, bảo mật được nâng cao cho đến phí xử lý thấp và ít lỗi hơn. Tuy nhiên, blockchain vẫn có những ưu điểm và nhược điểm:

- Ưu điểm:

+ Cải thiện độ chính xác bằng cách loại bỏ sự tham gia của con người vào quá trình xác minh.

+ Giảm thiểu chi phí bằng cách loại bỏ quá trình xác minh của bên thứ ba.

+ Tính phi tập trung làm cho việc giả mạo trở nên khó hơn.

+ Giao dịch an toàn, riêng tư và hiệu quả.

+ Công nghệ minh bạch.

+ Cung cấp giải pháp thay thế ngân hàng và cách để bảo mật thông tin cá nhân cho công dân của các quốc gia có chính phủ không ổn định hoặc kém phát triển.

- Nhược điểm:

+ Chi phí công nghệ đáng kể liên quan đến việc khai thác Bitcoin.

+ Giao dịch thấp mỗi giây.

+ Lịch sử sử dụng cho các hoạt động bất hợp pháp, như "Dark Web"

+ Quy định thay đổi tuỳ theo thẩm quyền và vẫn không chắc chắn.

+ Lưu trữ dữ liệu bị giới hạn.

Blockchain mang lại nhiều ưu điểm quan trọng, nhưng cũng đối mặt với những thách thức cần được vượt qua để đảm bảo sự phát triển bền vững trong tương lai. Sự tiếp tục nghiên cứu và phát triển là quan trọng để giải quyết những vấn đề này và tối ưu hóa lợi ích của blockchain trong nhiều lĩnh vực khác nhau.

## Smart Contract

### Định nghĩa

Hợp đồng thông minh (Smart contract) là một giao thức giao dịch dựa trên công nghệ blockchain. Tương tự như hợp đồng truyền thống, hợp đồng thông minh bao gồm đầy đủ những điều kiện theo thỏa thuận. Tuy nhiên, điều khoản trên hợp đồng thông minh được viết bằng ngôn ngữ lập trình dựa trên công nghệ blockchain.

Hợp đồng thông minh hiểu đơn giản là việc các chương trình được lưu trữ trên blockchain chạy khi thỏa mãn những điều kiện xác định từ trước.

### Cơ chế hoạt động

Smart contract hoạt động bằng cách tuân theo quy tắc câu lệnh “if/else” đơn giản, được viết thành mã trên chuỗi khối.

Một mạng máy tính thực hiện các hành động khi điều kiện xác định trước đó được đáp ứng và xác minh. Những hành động này bao gồm việc giải ngân cho người thích hợp, đăng ký phương tiện, gửi thông báo hoặc xuất vé,...

Sau đó, hợp đồng thông minh blockchain sẽ cập nhật khi giao dịch hoàn tất. Điều đó có nghĩa là giao dịch không thể thay đổi và chỉ những bên đã được cấp phép mới có quyền xem kết quả.

Trong một hợp đồng thông minh, có thể đặt ra nhiều quy định cần thiết để làm hài lòng những người tham gia và cam kết rằng nhiệm vụ sẽ được hoàn thành thỏa đáng.

Để thiết lập điều khoản, người tham gia phải xác định cách các giao dịch và dữ liệu của họ thể hiện trên blockchain, đồng ý về quy tắc “nếu/khi…thì…” chi phối những giao dịch đó, liệt kê tất cả trường hợp ngoại lệ có khả năng xảy ra và xác định khuôn khổ để giải quyết tranh chấp.

Sau đó, hợp đồng thông minh được lập trình bởi nhà phát triển. Hiện nay, cấu trúc của smart contract cũng phần nào được đơn giản hóa bởi nhiều tổ chức cung cấp dịch vụ blockchain cho doanh nghiệp tạo ra các mẫu, giao diện web và nhiều công cụ trực tuyến khác.

### Lợi ích của smart contract

**Tốc độ, hiệu quả và độ chính xác**

Khi một điều kiện đáp ứng đầy đủ, hợp đồng sẽ được thực hiện ngay lập tức. Hợp đồng thông minh là hợp đồng kỹ thuật số và hoàn toàn tự động, các bên tham gia không cần xử lý thủ tục giấy tờ, không mất thời gian điều chỉnh lỗi (thường xảy ra do soạn tài liệu theo cách thủ công).

**Sự tin cậy và minh bạch**

Vì không có bên thứ ba liên quan và hồ sơ giao dịch được mã hóa, chia sẻ giữa những người tham gia nên thông tin không thể bị thay đổi vì lợi ích cá nhân.

**Bảo vệ**

Hồ sơ giao dịch trên blockchain được mã hóa nên rất khó bị hack. Hơn nữa, vì mỗi bản ghi được kết nối với các bản ghi trước đó và tiếp theo trên sổ cái phân tán, tin tặc sẽ phải thay đổi toàn bộ chuỗi để thay đổi một bản ghi duy nhất.

**Tiết kiệm**

Hợp đồng thông minh loại bỏ nhu cầu sử dụng bên thứ ba để xử lý giao dịch. Nhờ đó, những bên tham gia tiết kiệm chi phí liên quan, cũng như giảm lãng phí thời gian.

## Một số nền tảng phổ biến

Hiện nay, có nhiều nền tảng blockchain phổ biến với mỗi nền tảng có đặc điểm riêng, hướng tiếp cận và ứng dụng khác nhau. Dưới đây là một số nền tảng blockchain phổ biến:

* Ethereum: Ethereum là một nền tảng blockchain phổ biến cho phép việc xây dựng các ứng dụng phi tập trung (DApps) và smart contracts.
* Cung cấp khả năng tạo các token chuẩn (ERC-20, ERC-721, v.v.) và là nền tảng của nhiều dự án DeFi và các ứng dụng phi tập trung khác.
* Bitcoin: Bitcoin là nền tảng blockchain đầu tiên và phổ biến nhất, được sử dụng cho việc chuyển tiền trực tuyến và lưu trữ giá trị.
* Cung cấp tính an toàn và minh bạch cho các giao dịch tiền điện tử.
* Binance Smart Chain (BSC): Binance Smart Chain là một nền tảng blockchain song song với Binance Chain, được sử dụng cho việc phát triển DApps và các dịch vụ tài chính phi tập trung. BSC đang trở nên phổ biến trong DeFi vì chi phí giao dịch thấp và khả năng tương tác tốt với hệ thống Binance Exchange.
* Cardano: Cardano là một nền tảng blockchain có độ tin cậy cao và chú trọng vào bảo mật và tính mở rộng. Được xây dựng bằng cách sử dụng nhiều lớp phân cấp để tăng cường khả năng mở rộng và tính bảo mật.
* Polygon (Matic): Polygon (trước đây được gọi là Matic Network) là một lớp phụ (layer-2) cho Ethereum, giúp tăng cường khả năng mở rộng và giảm chi phí giao dịch. Được sử dụng cho các ứng dụng blockchain với tốc độ và chi phí giao dịch thấp hơn.
* Solana: Solana là một nền tảng blockchain có khả năng xử lý giao dịch với tốc độ cao và có khả năng mở rộng. Được xây dựng để hỗ trợ các ứng dụng phi tập trung có độ phức tạp cao.
* Tezos: Tezos là một nền tảng blockchain dựa trên độ chủ quyền, cho phép người dùng tham gia vào việc đưa ra quyết định về cải thiện nền tảng.

### NEAR Protocol

NEAR Protocol là một blockchain hoạt động theo cơ chế public proof of stake và sharded (phân đoạn). Đây giống như một nền tảng đám mây do cộng đồng điều hành, có khả năng mở rộng cao và chi phí thấp dành cho các nhà phát triển để tạo ra các ứng dụng phi tập trung dễ dàng.

NEAR đủ an toàn để quản lý các tài sản có giá trị cao như tiền bạc hoặc danh tính và đủ hiệu suất để làm cho chúng hữu ích, đặc biệt là sức mạnh của Open Web vào tay người dùng.

Các công nghệ cốt lõi của Near

* Sharding: Hệ thống được thiết kế để phân phối tính toán trên nhiều phân đoạn song song.
* Sự đồng thuận: Đạt được sự đồng thuận trên tất cả các [**node**](https://coin98.net/node-la-gi) thông qua việc sử dụng thuật toán mới là Nightshade.
* Staking selection & Game theory: Để tham gia vào quá trình xác thực, các staker được lựa chọn bằng cách sử dụng một quy trình ngẫu nhiên an toàn, giúp phân phối tối ưu không gian giữa các bên và cung cấp các động lực để họ hoạt động với hành vi tốt.
* Tính ngẫu nhiên: Cách tiếp cận ngẫu nhiên không thể đoán trước được.

### ReactJS

ReactJS là một thư viện JavaScript phổ biến được sử dụng để xây dựng giao diện người dùng hiệu quả và linh hoạt. Được phát triển bởi Facebook, ReactJS chủ yếu tập trung vào việc xây dựng các ứng dụng web động và tương tác, nơi mà dữ liệu thay đổi liên tục mà không cần phải tải lại trang.

Một trong những đặc điểm nổi bật của ReactJS là sử dụng khái niệm "component", cho phép phân chia giao diện người dùng thành các thành phần nhỏ, dễ quản lý và tái sử dụng. Điều này giúp tăng cường sự cấu trúc của mã nguồn, làm cho việc phát triển và bảo trì ứng dụng trở nên thuận tiện.

ReactJS còn nổi tiếng với khả năng tương thích cao, có thể tích hợp dễ dàng với nhiều thư viện và framework khác. Nó cũng sử dụng Virtual DOM (Document Object Model ảo) để tối ưu hóa hiệu suất của ứng dụng, giảm thiểu việc làm mới lại DOM thực tế, điều này giúp cải thiện trải nghiệm người dùng.

### NodeJS

Node.js là một nền tảng phát triển dựa trên JavaScript, được xây dựng trên engine V8 của Google Chrome, cho phép chúng ta xây dựng ứng dụng máy chủ hiệu quả và có khả năng mở rộng. Node.js đặt trọng tâm vào việc xử lý sự kiện và non-blocking I/O, làm cho nó trở thành lựa chọn lý tưởng cho việc xây dựng ứng dụng thời gian thực và ứng dụng đa người dùng.

Một trong những đặc điểm nổi bật của Node.js là khả năng chia sẻ mã nguồn giữa phía máy chủ và phía client, nhờ sự đồng nhất của JavaScript trên cả hai môi trường. Điều này giúp giảm độ phức tạp và tăng tốc quá trình phát triển.

Node.js cũng hỗ trợ npm (Node Package Manager), một kho lưu trữ rất lớn với các gói mã nguồn mở, giúp đơn giản hóa quá trình quản lý dependencies và modules trong ứng dụng.

Ngoài ra, Node.js cũng thích hợp cho việc xây dựng các ứng dụng real-time như ứng dụng trò chơi trực tuyến, ứng dụng chat và các dịch vụ web có yêu cầu độ trễ thấp.

### MongoDB

MongoDB là một hệ quản trị cơ sở dữ liệu phi quan hệ (NoSQL) phổ biến, được thiết kế để lưu trữ và truy xuất dữ liệu trong các ứng dụng hiện đại. Đặc biệt, MongoDB sử dụng mô hình dữ liệu JSON-like (BSON), cung cấp sự linh hoạt và hiệu suất cho các ứng dụng có cấu trúc dữ liệu đa dạng.

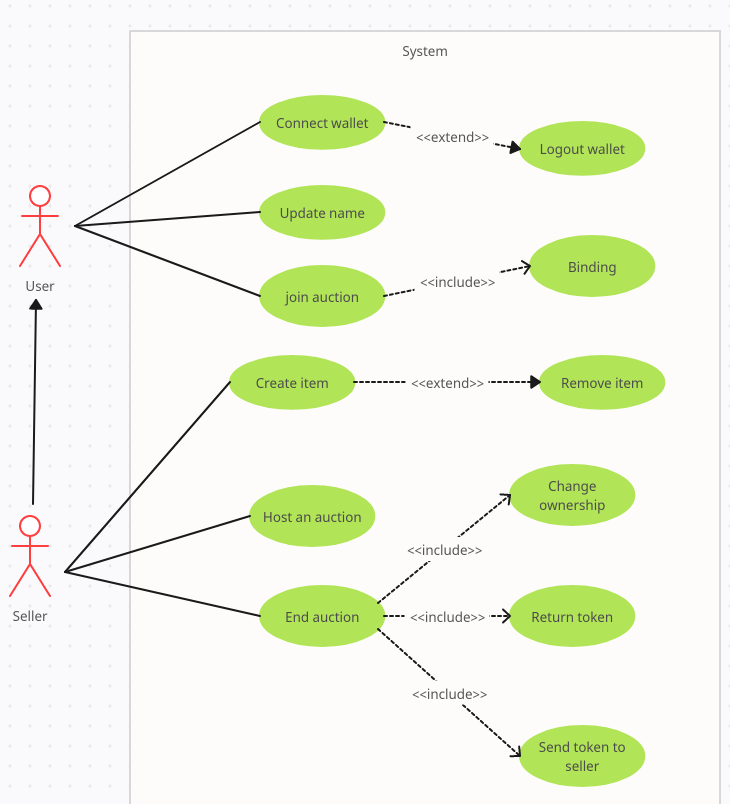
Một trong những điểm mạnh của MongoDB là khả năng lưu trữ dữ liệu dưới dạng tài liệu (document), thay vì bảng và hàng như trong cơ sở dữ liệu quan hệ. Điều này giúp MongoDB dễ dàng mở rộng và thích hợp cho các ứng dụng với yêu cầu dữ liệu thay đổi linh hoạt.

MongoDB cũng hỗ trợ các tính năng như replica set và sharding, giúp tăng cường khả năng mở rộng và đảm bảo tính sẵn sàng cao cho hệ thống.

Ngoài ra, MongoDB được tích hợp chặt chẽ với ngôn ngữ lập trình JavaScript thông qua sử dụng BSON, cho phép nhà phát triển xây dựng ứng dụng từ phía máy chủ đến phía client với một ngôn ngữ duy nhất.

# PHÂN TÍCH VÀ THIẾT KẾ

## Sơ đồ Use case tổng quát



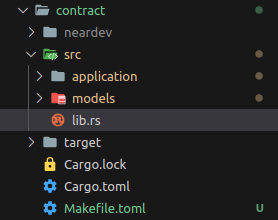
Hình 1 Sơ đồ use case tổng quát

## Tổng quan về mô hình ứng dụng công nghệ blockchain vào hệ thống

## 

Hình 2 Mô hình ứng dụng

## Xây dựng smart contract



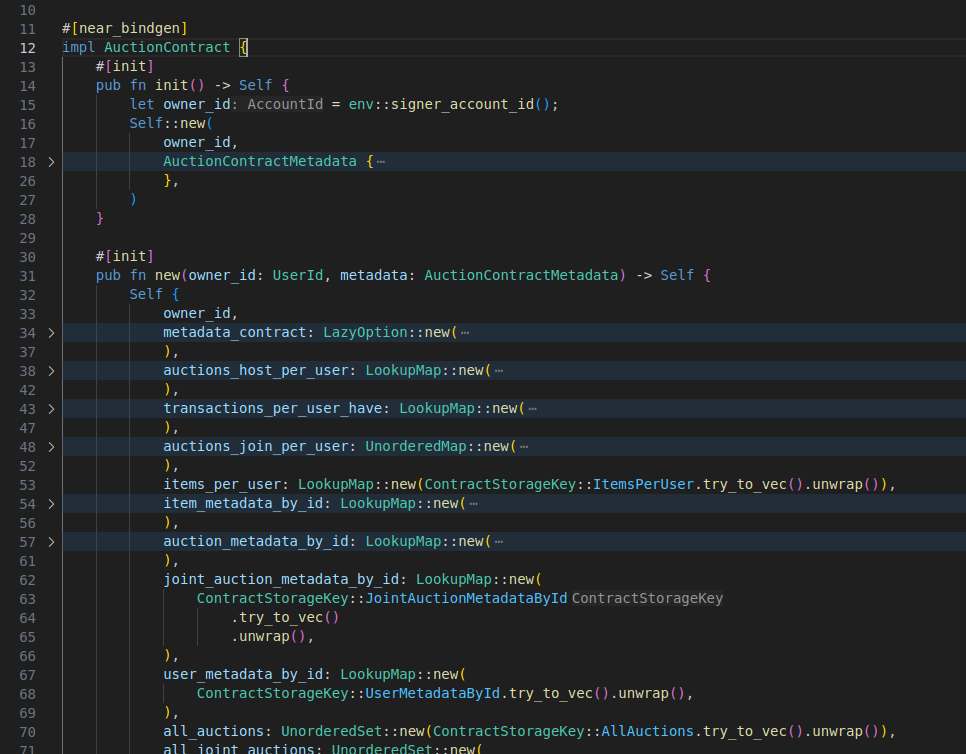
Hình 3 Cấu trúc smart contract

Dữ liệu sẽ được lưu trên blockchain thông qua các giao dịch dựa trên smart contract

Cây thư mục của smart contract sẽ bao gồm những thành phần chính sau:

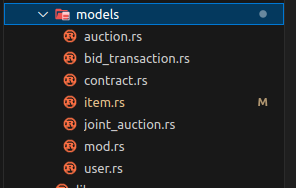
* File lib.rs: Đây là file chính trong một dự án smart contract của Near Protocol. Nó chứa mã nguồn chính của smart contract và thường là nơi bạn định nghĩa các hàm và logic cụ thể của smart contract. File lib.rs thường chứa hàm #[init] (hoặc tương tự) được gọi khi smart contract được triển khai lần đầu tiên.
* Thư mục application: Chứa các file hiện thực các phương thức của hệ thống.
* Thư mục models: Chứa các struct của các đối tượng trong hệ thống, được sử dụng để khởi tạo các thực thể.
* Thư mục target trong một dự án Rust là nơi chứa các tập tin và thư mục tạm thời được tạo ra trong quá trình biên dịch mã nguồn.
* Thư mục neardev chứa file lưu trữ địa chỉ của smart contract.

## 



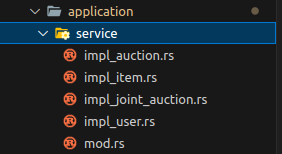
Hình 4 Khởi tạo smart contract trong file lib.rs

Bắt đầu khởi tạo smart contract trong file lib.rs. Phương thức init sẽ khai báo những thông số mặc định của smart contract. Các thông số khởi tạo của hệ thống sẽ được khai báo trong phương thức new.



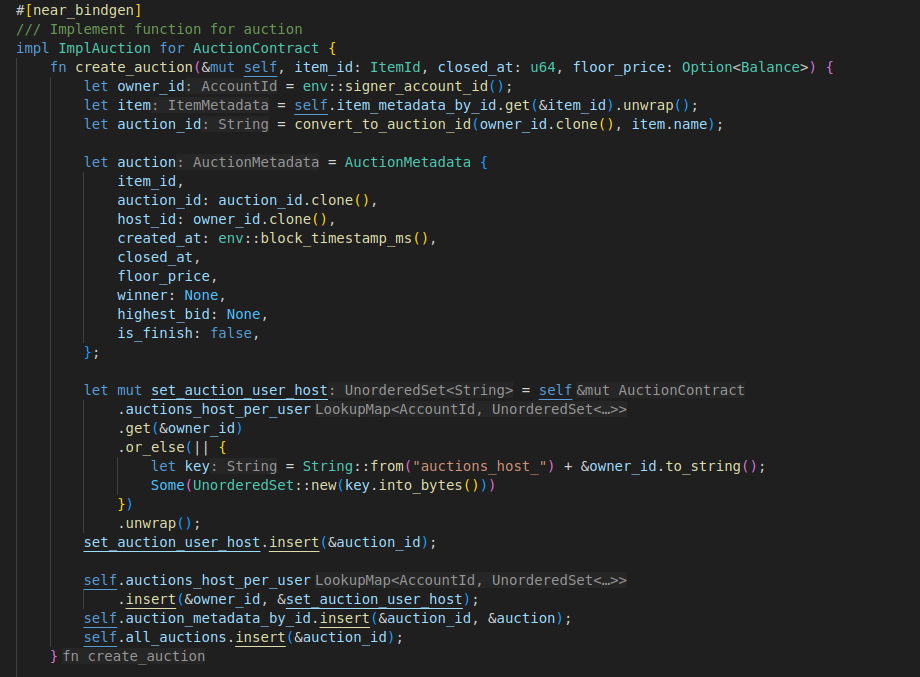
Hình 5 Tạo các struct

Sau khi đã khởi tạo smart contract, nhóm sẽ tiến hành khởi tạo các struct cho hệ thống.



Hình 6 Hiện thực các phương thức đã khai báo

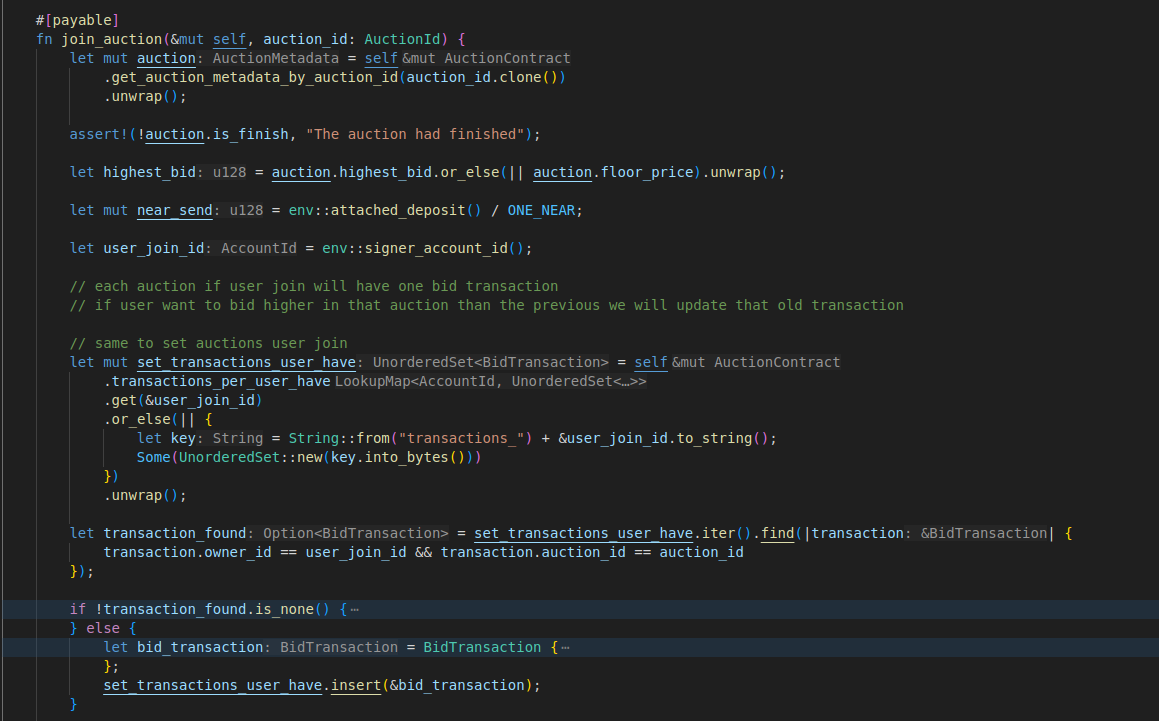
Hiện thực những phương thức đã được khai báo trong file lib.rs. Nhóm sẽ chia nhỏ các module chức năng theo nhóm thành phần để dễ dàng quản lý code. Ví dụ trong "impl\_auction.rs" sẽ chứa những phương thức liên quan đến tạo các cuộc đấu giá, quản lý trạng thái các cuộc đấu giá. Trong "impl\_users.rs" sẽ chứa các phương thức liên quan đến nguời dùng như các giao dịch.



Hình 7 Tạo cuộc đấu giá

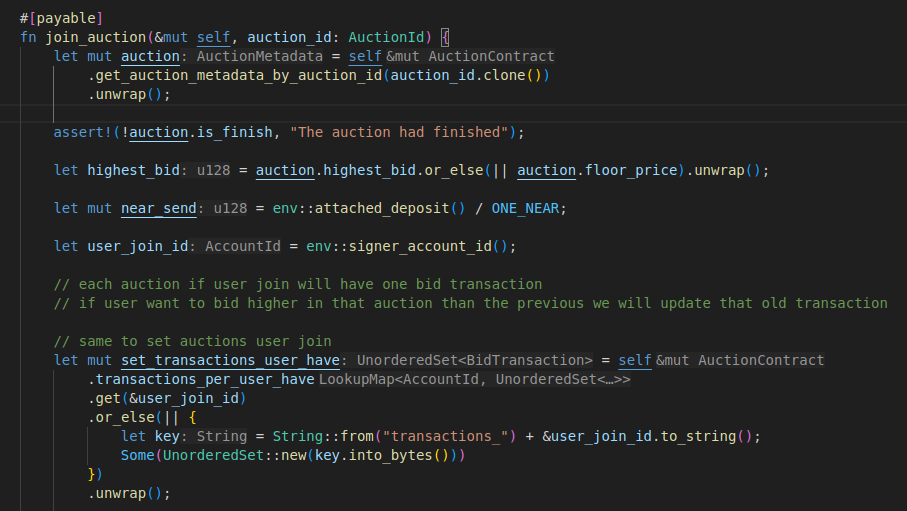
Chức năng quan trọng đầu tiên của hệ thống chính là tạo ra cuộc đấu giá. Sau khi đã tạo sản phẩm, người dùng sẽ có thể mở một cuộc đấu giá. Để có thể tạo được một cuộc đấu giá, một số thông tin cần phải có như: sản phẩm, giá khởi điểm và thời gian diễn ra. Cuộc đấu giá ban đầu sẽ có trạng thái của "is\_finished" là false, thuộc tính này dùng để kiểm tra xem cuộc đấu giá còn diễn ra hay không. Một thông số quan trọng khác là "closed\_at", nó sẽ cho những người dùng biết được cuộc đấu giá sẽ kết thúc lúc nào.

Trong lúc cuộc đấu giá diễn ra, những người dùng khác có thể tham gia vào. Để tham gia vào, họ sẽ phải đặt cược một số tiền cao hơn số tiền hiện tại của sản phẩm.



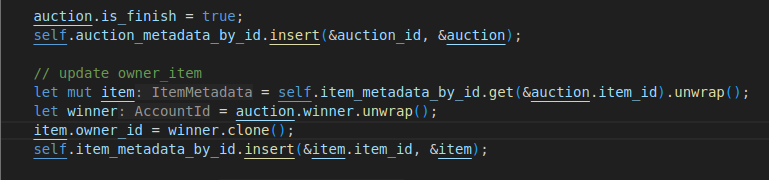
Hình 8 Phương thức để người dùng tham gia vào một cuộc đấu giá

Để dễ dàng trong việc thanh toán và giao dịch, nhóm đã quyết định sử dụng token của NEAR để làm phương tiện thanh toán. Mỗi khi người dùng thực hiện một giao dịch, hệ thống sẽ yêu cầu bỏ vào một lượng token tương ứng. Để làm được hành động này, nhóm đã sử dụng macro #[payable]. Nó sẽ bắt buộc phải có token để thực hiện được phương thức.



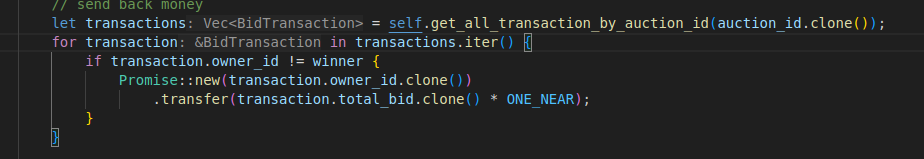
Hình 9 Phương thức cho người dùng tham gia cuộc đấu giá

Sau khi cuộc đấu giá kết thúc, người có mức cược cao nhất sẽ chiến thắng, họ sẽ được quyền sở hữu món đồ đó. Những người dùng khác sẽ được hoàn lại số tiền mà họ đã bỏ ra. Để hiện thực chức năng này, cần phải thực hiện được hai vấn đề chính là đổi quyền sở hữu của item và chuyển lại số tiền tương ứng cho những người không giành chiến thắng.



Hình 10 Kết thúc cuộc đấu giá

Khi kết thúc cuộc đấu giá, đầu tiên chúng ta phải cập nhật trạng thái cho cuộc đấu giá bằng cách thiết lập thuộc tính "is\_finished" là true. Sau đó tiến hành thực hiện việc chuyển quyền sở hữu bằng cách thay đổi "owner\_id" thành id của người thắng cuộc.



Hình 11 Trả lại số tiền tương ứng cho những người không thắng

Thực hiện chuyển lại số tiền cho những người không thắng trong cuộc đấu giá. Để thực hiện công việc này, tiến hành lăp qua danh sách chứa các giao dịch trước đó (các giao dịch đấu giá) và thực hiện chuyển lại với số tiền tương ứng.



Hình 12 Chuyển số tiền cho người bán

Cuối cùng sẽ là bước chuyển tiền cho người bán sản phẩm đó.

# THỰC NGHIỆM

## Cài đặt thực nghiệm

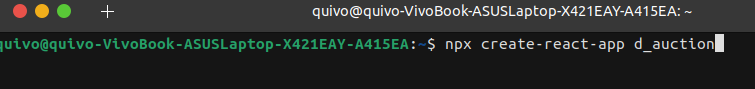
* Môi trường thực nghiệm: Windows 11
* Đối với hệ điều hành Windows, ta nên sử dụng Windows Subsystem for Linux 2 (WSL2)

<https://docs.microsoft.com/en-us/windows/wsl/install-manual#downloading-distros>.

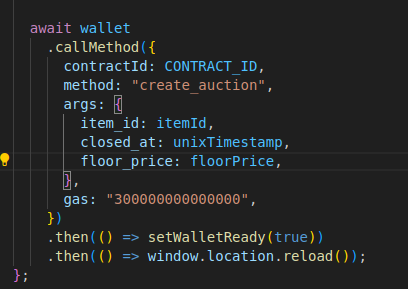
* Sau khi cài đặt xong mở WSL và tiến hành
* Cài đặt NodeJS (nên sử dụng phiên bản 18.19.0) ở đường dẫn sau https://nodejs.org/en/download/package-manager/
* Cài đặt NEAR CLI bằng gõ lệnh sau ở WSL: npm install -g near-cli
* Cài đặt Rust (nếu cần) ở đường dẫn sau [Install Rust - Rust Programming Language (rust-lang.org)](https://www.rust-lang.org/tools/install)

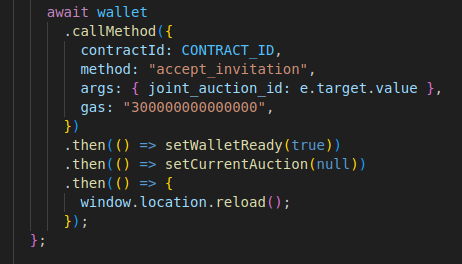
- Frontend

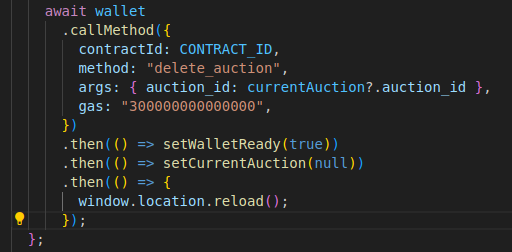
* Cài đặt npm: sudo apt install npm
* Tạo dự án Reactjs

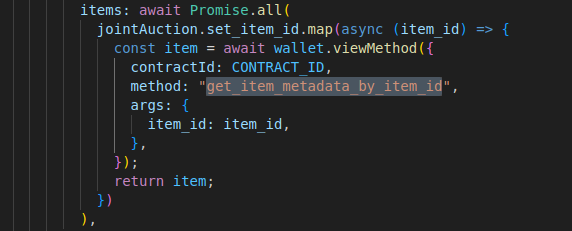


* Xây dựng giao diện cho trang web
* Sử dụng các api từ smart contract



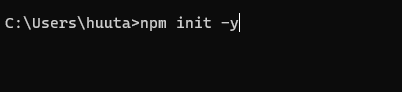


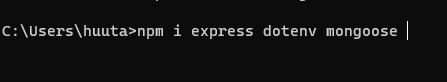




- Backend

* Tạo dự án với nodejs và một số thư viện (express, mongoose,.. )





* Định nghĩa model cho ứng dụng
  + User



* + Product



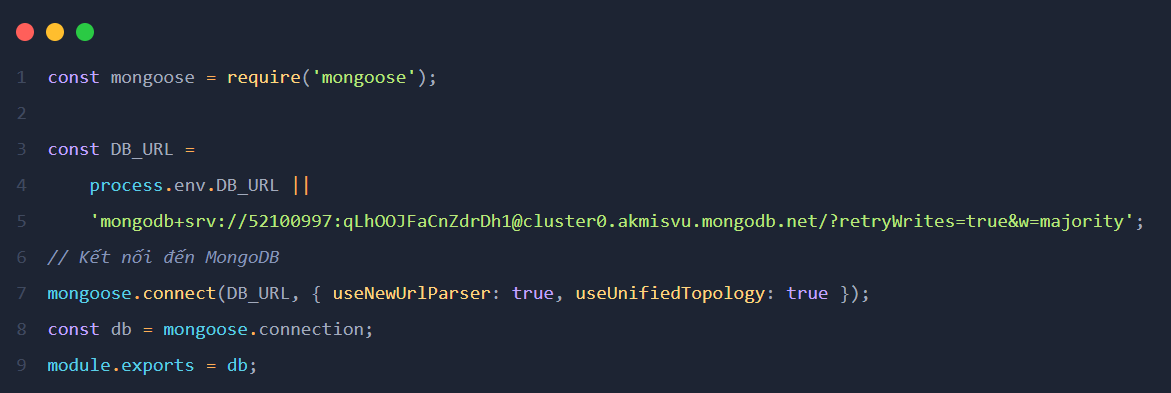
* Định tuyến router cho API



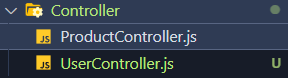




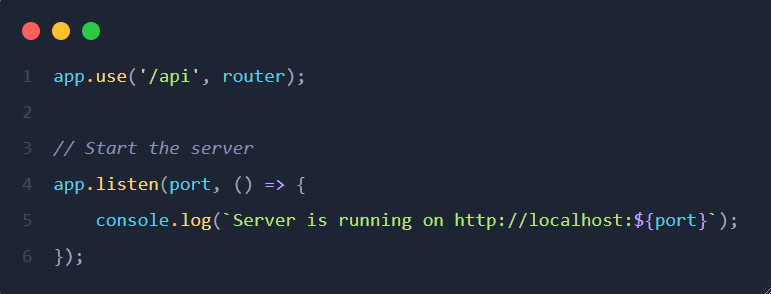
* Cấu hình kết nối với server với MongoDB



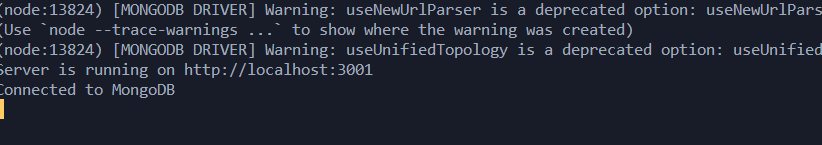
* Định nghĩa các method xử lý request



* Khởi tạo server



* Khởi chạy server và xem kết quả



* Ở môi trường development, ta có thể triển khai contract trên localnet hoặc testnet.

### Localnet

* Hướng dẫn chi tiết: [Creating a Local Development Environment | NEAR Documentation](https://docs.near.org/develop/testing/kurtosis-localnet)
* Cài đặt
* Docker (https://docs.docker.com/get-docker/)
* NEAR CLI
* Yarn (<https://classic.yarnpkg.com/lang/en/docs/install>)
* Kurtosis CLI (https://docs.kurtosis.com/install)
* Các bước thực hiện:

1. Chạy Docker
2. Chạy lệnh sau trên terminal để tải file script về máy

curl -o ~/launch-local-near-cluster.sh https://raw.githubusercontent.com/kurtosis-tech/near-package/master/launch-local-near-cluster.sh -L

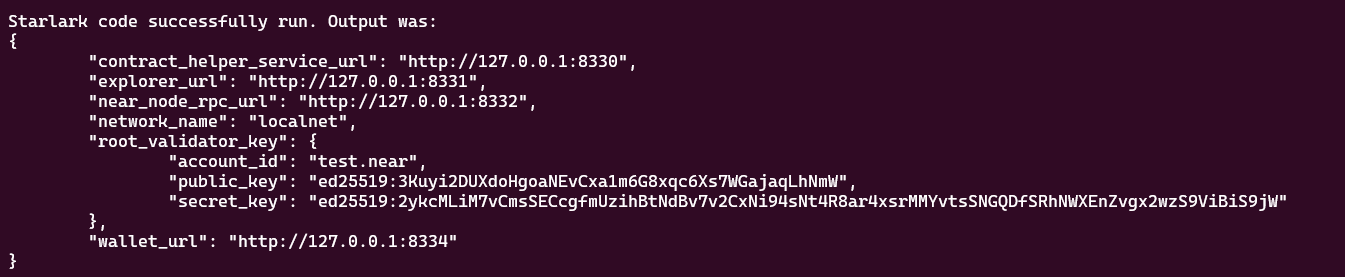
1. Cấp quyền ghi cho file script vừa tải về thông qua lệnh sau

chmod u+x ~/launch-local-near-cluster.sh

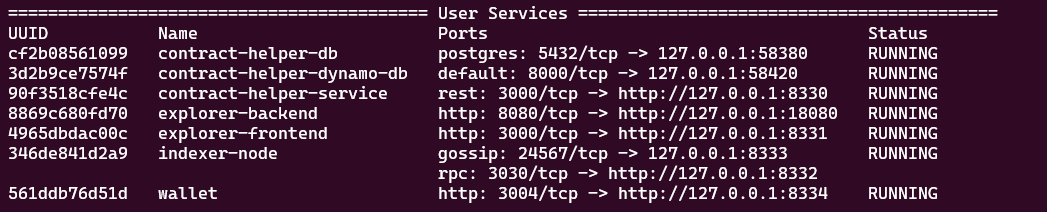
1. Chạy Kurtosis NEAR Package thông qua lệnh

~/launch-local-near-cluster.sh

Sau khi chạy, terminal sẽ log ra rất nhiều thông tin tuy nhiên ta chỉ quan tâm đến



Đây là thông tin của localnet lưu lại các thông tin này để có thể kết nối frontend với localnet

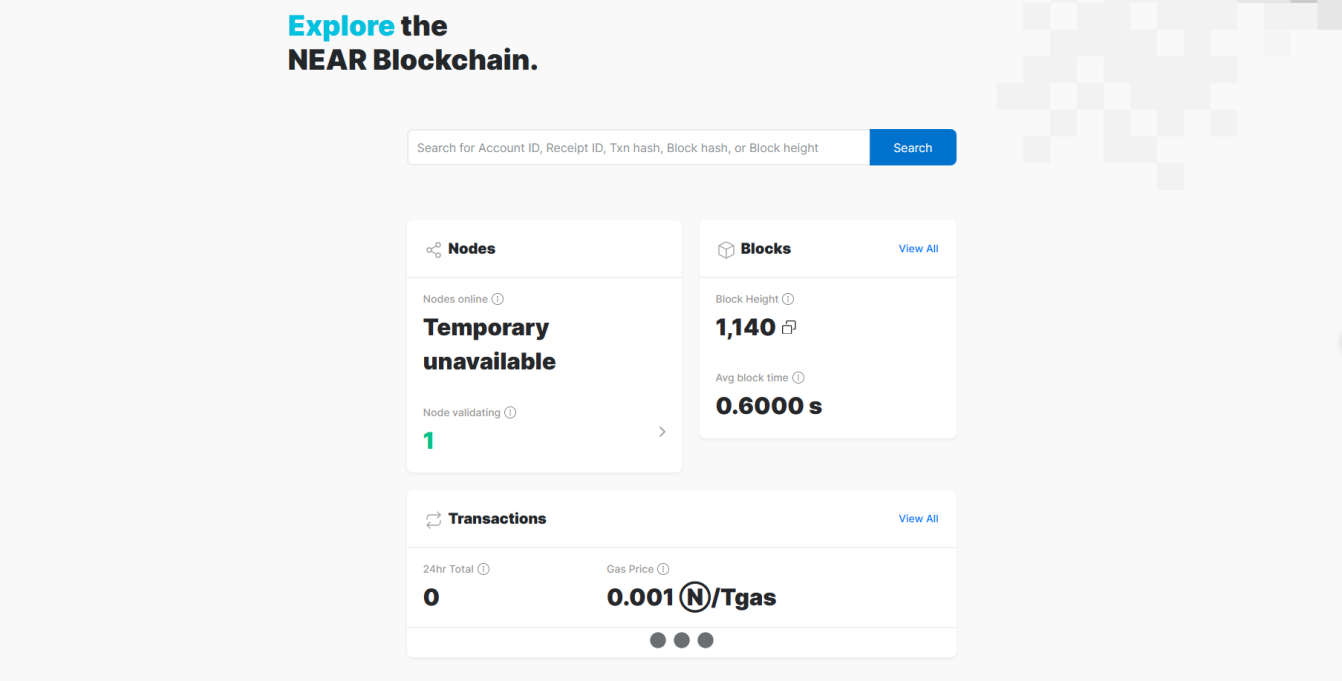


Đây là port của các service



Để chạy NEAR CLI cho localnet, ta gõ lệnh theo hướng dẫn.

* Explorer: http://127.0.0.1:8331



Ta thấy có 1 node validating đó chính là máy tính của chúng ta.

* Wallet: http://127.0.0.1:8334

### Testnet

* Không cần cài đặt gì cả. Network mặc định của NEAR CLI là testnet.
* Explorer: <https://explorer.testnet.near.org/> để theo dõi các transaction,...
* Wallet: https://testnet.mynearwallet.com/

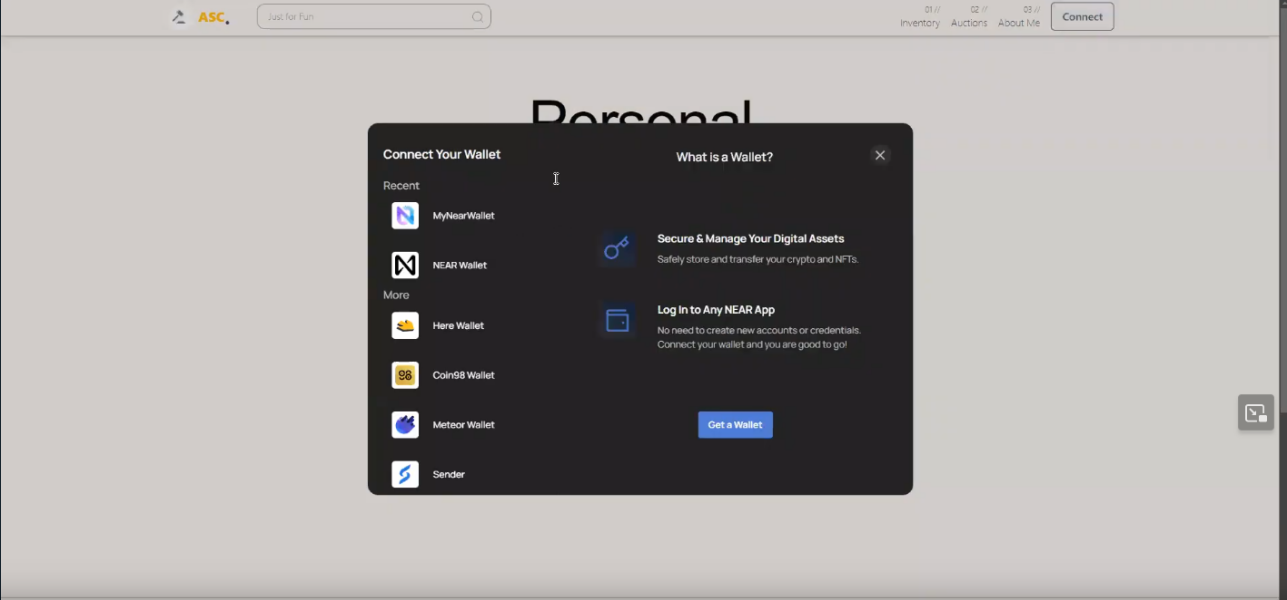
## Kết quả thực nghiệm

Sau thời gian hiện thực dự án, nhóm đã phát triển được một trang web với các chức năng cho phép người dùng có thể thực hiện đấu giá qua hệ thống, từ việc tạo cuộc đấu giá cho đến tham gia đấu giá. Trang web với giao diện thân thiện và cách sử dụng đơn giản giúp người dùng có thể dễ dàng tiếp cận

## 

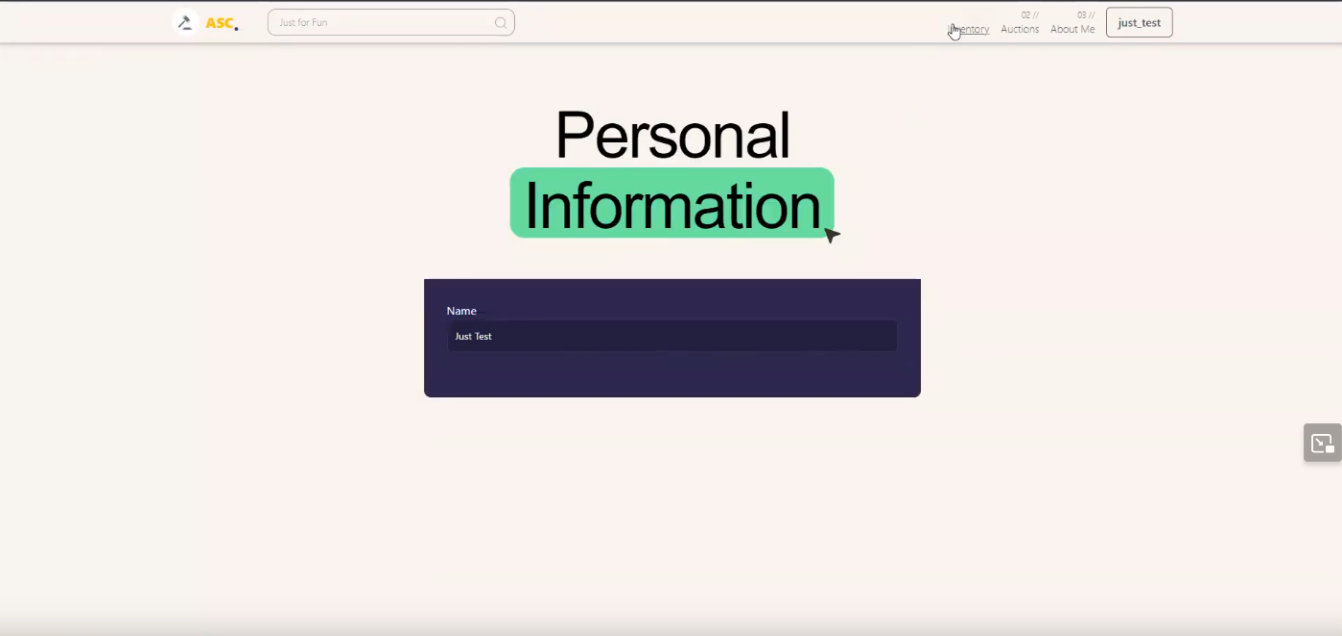
Hình 13 Trang chủ của website

Để sử dụng được hệ các chức năng của trang web, người dùng phải liên kết ví NEAR để đăng nhập.

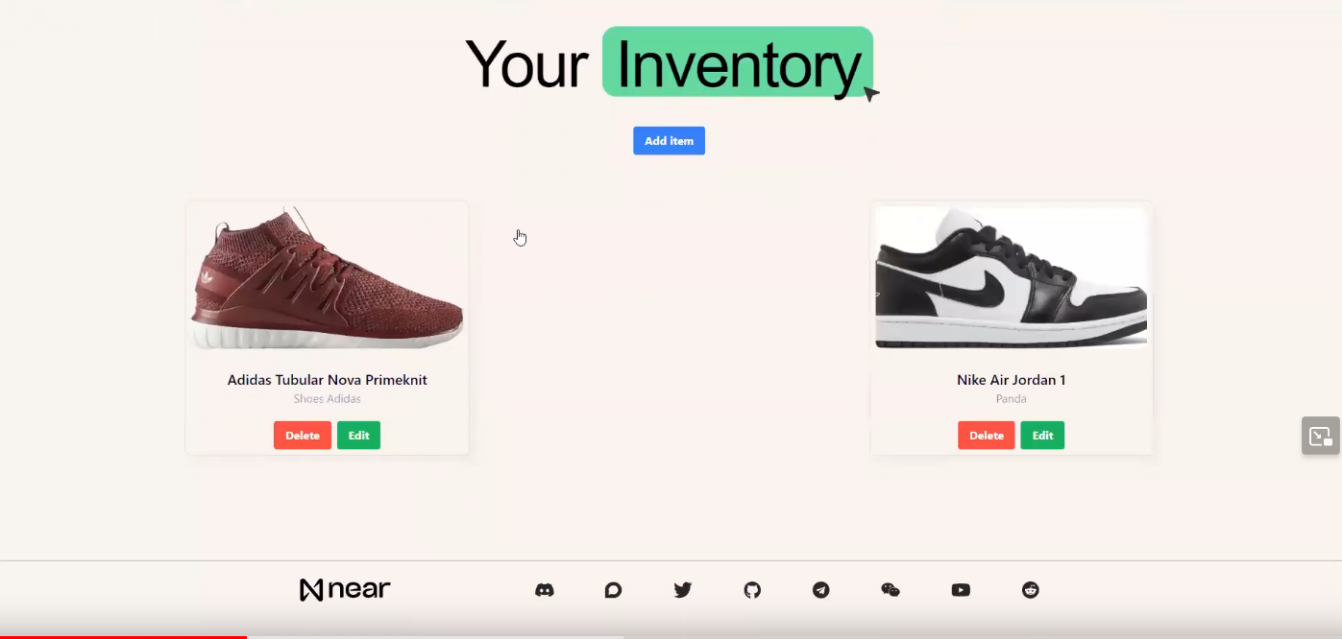


Hình 14 Liên kết ví

Sau khi liên kết ví, người dùng sẽ vào được hệ thống. Đầu tiên sẽ là trang thông tin. Ở đây người dùng có thể thay đổi tên hiển thị để làm định danh trong quá trình sử dụng trang web.

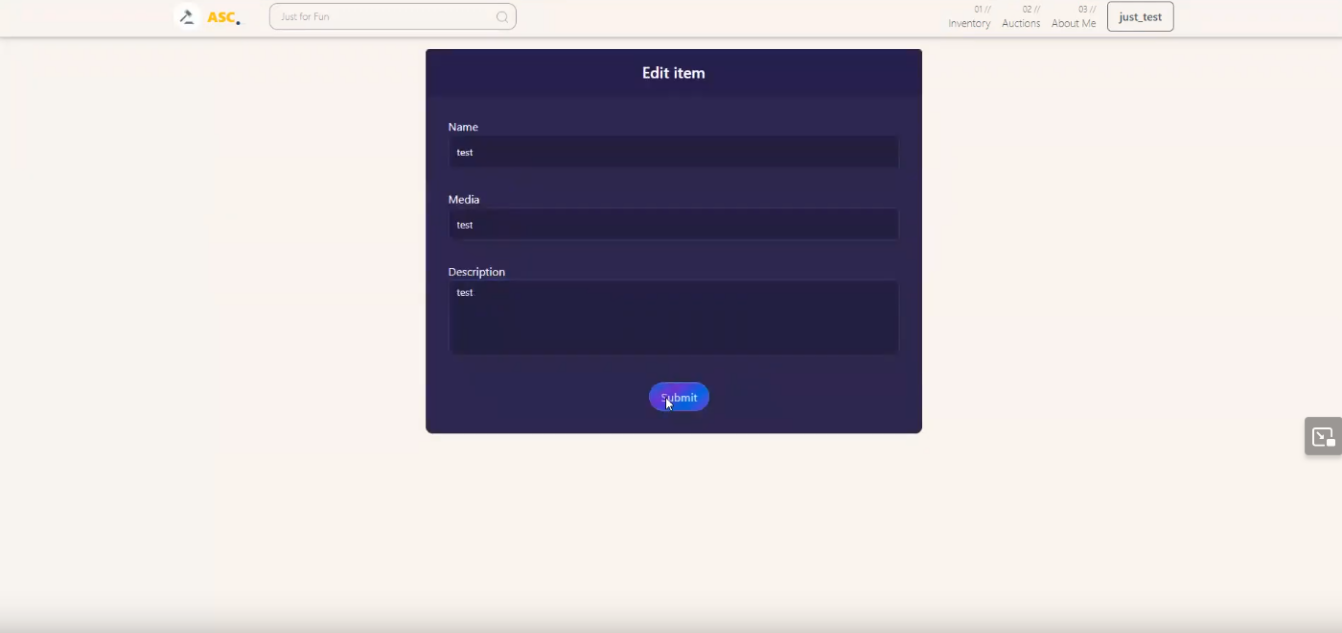


Hình 15 Trang thông tin

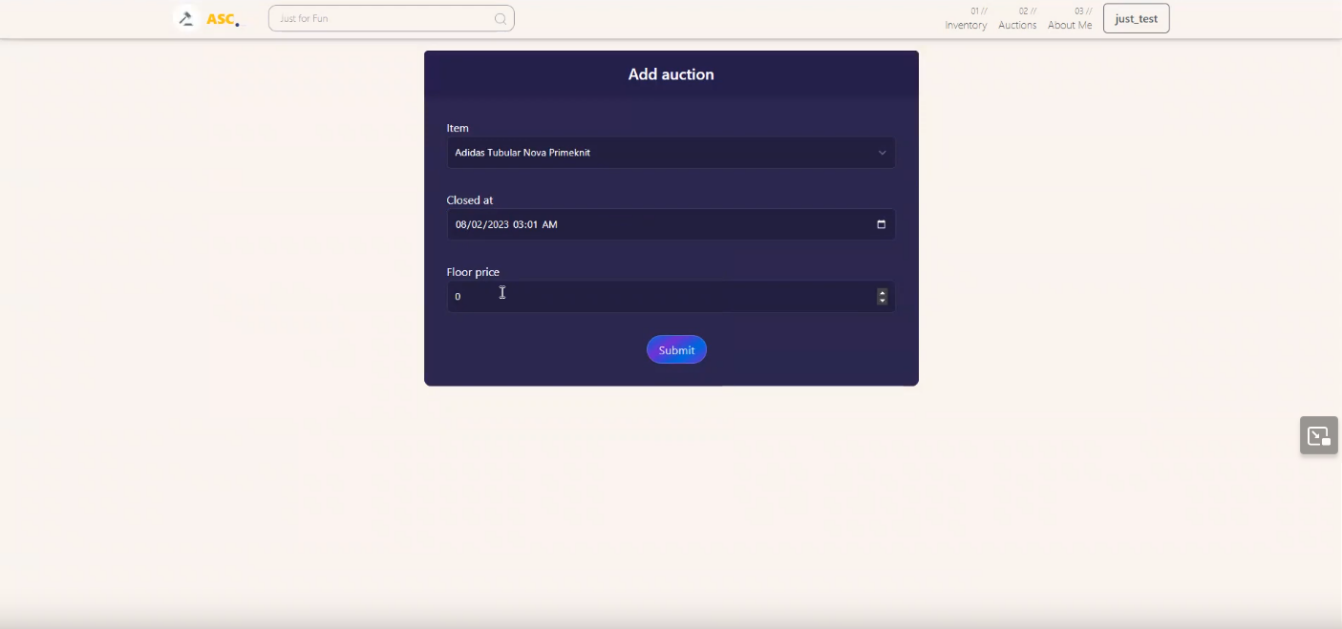


Hình 16 Giao diện chính

Tiếp theo sẽ là trang Inventory, tại đây người dùng có thể xem những sản phẩm của mình, từ nhũng sản phẩm này, người dùng có thể mở các cuộc đấu giá. Ngoài ra người dùng còn có thể tạo mới item bằng cách nhấn vào nút "Add Item".



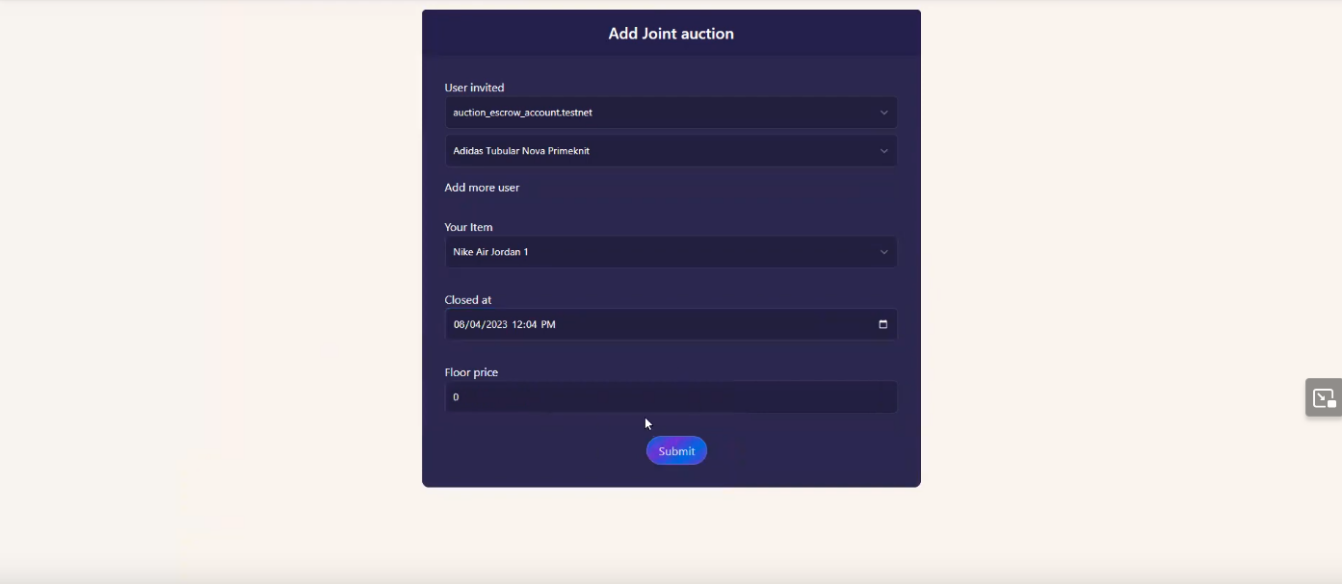
Hình 17 Giao diện tạo sản phẩm



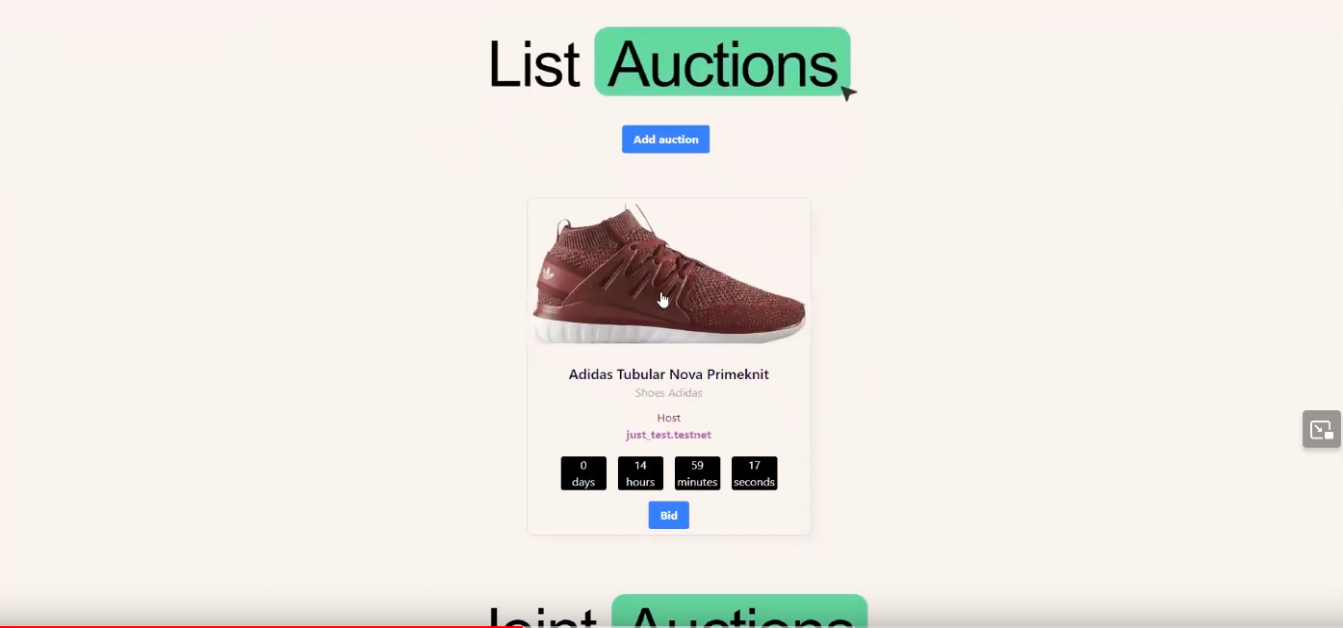
Hình 18 Giao diện tạo cuộc đấu giá

Tại đây người dùng sẽ khởi tạo một cuộc đấu giá. Người dùng sẽ phải nhập vào các thông số như sản phẩm, giá và thời gian kết thúc cuộc đấu giá.

Ngoài ra, người dùng còn có thể mời người khác cùng tổ chức đấu giá

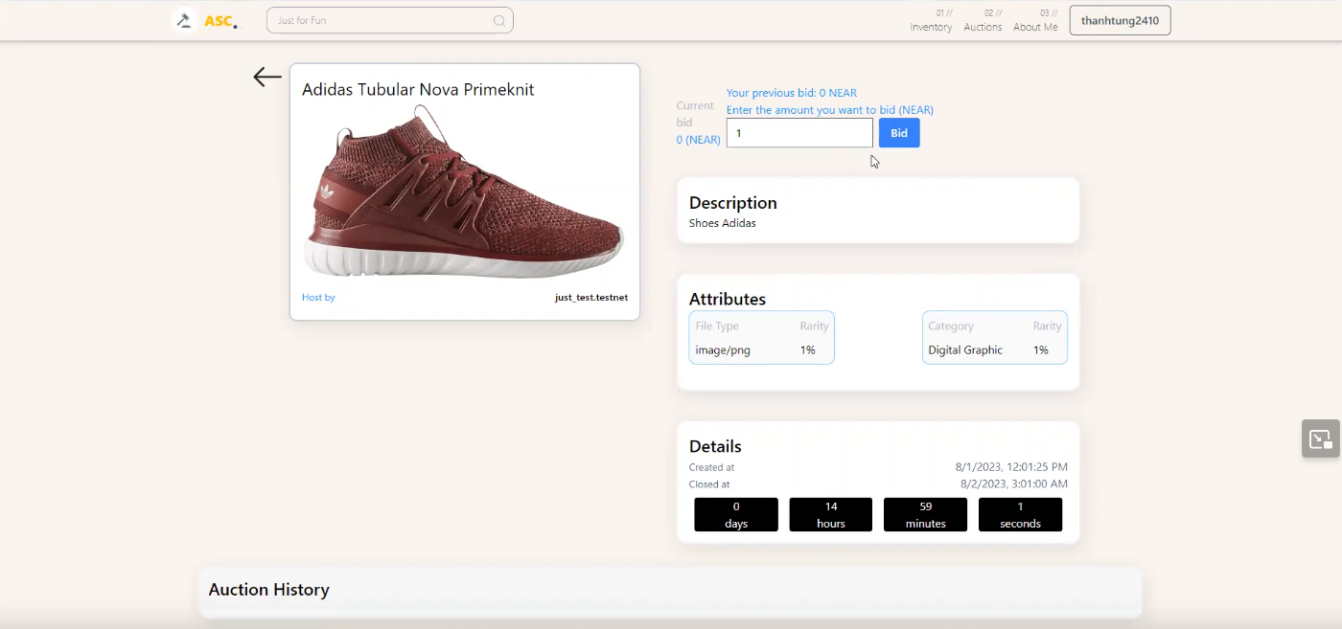


Hình 19 Giao diện mời người khác tham gia tổ chức



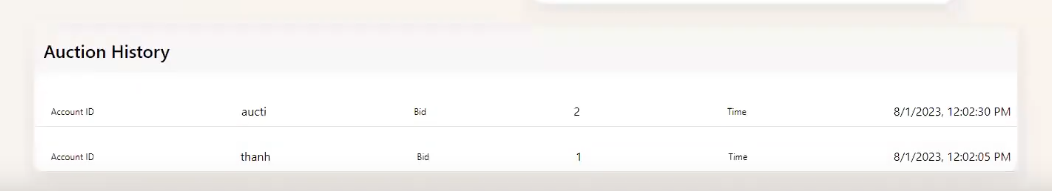
Hình 20 Giao diện xem các cuộc đấu giá đang diễn ra

Những cuộc đấu giá sau khi được khởi tạo và đang còn trong thời gian diễn ra thì sẽ được hiển thị tại đây, tất cả người dùng trong hệ thống sẽ thấy được sản phẩm này và có thể tham gia đấu giá bằng cách click vào cuộc đấu giá.



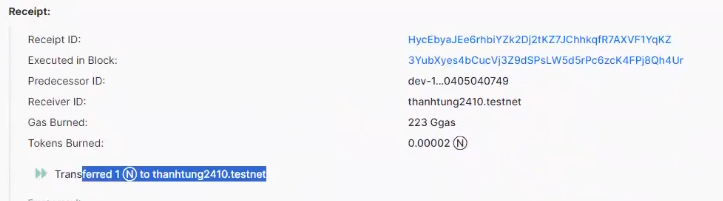
Hình 21 Giao diện đấu giá

Khi chọn vào một cuộc đấu giá thì người dùng sẽ xem được chi tiết của cuộc đấu giá.



Hình 22 Danh sách người tham gia đấu giá

Sau khi cuộc đấu giá kết thúc, số tiền của những người thua sẽ được hoàn trả về. Số tiền của người thắng cuộc thì sẽ được chuyển cho người chủ sở hữu cũ của sản phẩm đó.



Hình 23 Thông tin giao dịch

Ngoài ra trang thông tin còn cung cấp một tính năng quét mã QR để người dùng dễ dàng và thuận tiện hơn cho việc chia sẻ. Mã qr sẽ được sinh ra mỗi khi sản được trao đổi thành công, nó sẽ lưu thông tin của người sở hữu mới, thông tin của sản phẩm và giao dịch.



Hình 24 Mã QR

# KẾT LUẬN

## Kết luận

Đây là một sản phẩm với những chức năng cơ bản của hình thức đấu giá trực tuyến, với giao diện thân thiện và dễ sử dụng, trang web sẽ có thể dễ dàng tiếp cận với người dùng. Ngoài ra, dự án của này đã thành công trong việc việc kết hợp sức mạnh của lĩnh vực đấu giá trực tuyến với ưu điểm phi tập trung của blockchain, đặc biệt là sử dụng NEAR Protocol. Việc áp dụng blockchain đã mang lại tính minh bạch và an ninh đối với quá trình đấu giá, giúp ngăn chặn gian lận và đảm bảo tính chân thực của thông tin giao dịch.

Nhóm đã xây dựng một hệ thống đấu giá linh hoạt và dễ sử dụng, nơi mọi người có thể tham gia mà không cần phải tin tưởng vào bên trung gian. Sự tích hợp của NEAR Protocol đã cung cấp khả năng mở rộng và hiệu suất cao, đồng thời giảm thiểu chi phí giao dịch và thời gian xác nhận.

Ngoài ra, nhóm cũng đã đặc biệt chú trọng vào trải nghiệm người dùng, tạo ra một giao diện thân thiện và dễ sử dụng. Đồng thời, sự minh bạch của blockchain đã tạo ra một môi trường đáng tin cậy và an toàn cho cả người mua và người bán. Thông quan sản phẩm này, nhóm mong muốn mang công nghệ blockchain đến gần hơn với người dùng.

## Hướng phát triển

Với một sản phẩm có tính mở rộng cao, từ nền tảng hiện tại, hệ thống có thể nâng cấp lên về nhiều mặt:

* Tích Hợp Thêm Tính Năng: Mở rộng danh mục tính năng để tạo ra một trải nghiệm người dùng đa dạng và đầy đủ. Cụ thể, có thể xem xét việc thêm tính năng như đấu giá theo thời gian, đấu giá từ xa, hoặc tích hợp các phương thức thanh toán tiện lợi khác nhau.
* Phát Triển Ứng Dụng Di Động: Xây dựng ứng dụng di động để mở rộng sự tiện lợi và tiếp cận của người dùng. Ứng dụng di động có thể mang lại trải nghiệm linh hoạt và thuận tiện hơn cho người sử dụng.
* Nâng Cao Giao Diện Người Dùng: Tối ưu hóa giao diện người dùng để làm cho trang web trở nên dễ sử dụng hơn và thu hút nhiều người dùng hơn. Cải thiện trải nghiệm người dùng có thể bao gồm tối ưu hóa tốc độ tải trang, cải thiện công cụ tìm kiếm và thêm tính năng tương tác đặc sắc.
* Tăng Cường Bảo Mật: Tăng cường lớp bảo mật của hệ thống để đảm bảo an toàn cho dữ liệu và giao dịch. Có thể xem xét việc triển khai các biện pháp bảo mật cao cấp như xác thực hai yếu tố và mã hóa dữ liệu.
* Mở Rộng Hỗ Trợ Ngôn Ngữ và Quốc Gia: Nếu mục tiêu là phục vụ một lượng người dùng toàn cầu, hãy xem xét việc mở rộng hỗ trợ cho nhiều ngôn ngữ và quốc gia khác nhau. Điều này có thể cần sự hiểu biết sâu rộng về văn hóa và pháp lý của các thị trường khác nhau.

# TÀI LIỆU THAM KHẢO

**Tiếng Việt**

[20/12/2023]<https://advertisingvietnam.com/cach-thuc-hoat-dong-cua-blockchain-p20340>

[20/12/2023]<https://200lab.io/blog/uu-va-nhuoc-diem-cua-blockchain/>

[21/12/2023]<https://chat.openai.com>

[21/12/2023]<https://www.elcom.com.vn/hop-dong-thong-minh-la-gi-ung-dung-smart-contract-tren-blockchain-1694515090>

[21/12/2023]https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjVxa6bna2DAxXsklYBHcCSD9UQFnoECAgQAQ&url=https%3A%2F%2Fcoin98.net%2Fnear-protocol&usg=AOvVaw3pq5FL2b6BgYYx2sa8oU7g&opi=89978449

**Tiếng Anh**

[18/12/2023]<https://www.investopedia.com/terms/b/blockchain.asp>

[20/12/2023]<https://docs.near.org/>

[22/12/2023][Creating a Local Development Environment | NEAR Documentation](https://docs.near.org/develop/testing/kurtosis-localnet)