ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA CÔNG NGHỆ PHẦN MỀM

BÁO CÁO ĐỒ ÁN CUỐI KỲ

Môn học: Đồ án 2 – SE122.M21

ĐỀ TÀI:
NGHIÊN CỨU VÀ XÂY DỰNG HỆ THỐNG ĐẤU GIÁ VẬT PHẨM ERC-721 VÀ ERC-1155 TRÊN NỀN TẢNG ETHEREUM

Giảng viên hướng dẫn: ThS. Nguyễn Tấn Toàn

Sinh viên thực hiện: Nguyễn Đức Hướng 19521592

Ngô Dương Kha 19520117

TP HCM, 06/2022

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA CÔNG NGHỆ PHẦN MỀM

BÁO CÁO ĐỒ ÁN CUỐI KỲ

Môn học: Đồ án 2 – SE122.M21

ĐỀ TÀI:
NGHIÊN CỨU VÀ XÂY DỰNG HỆ THỐNG ĐẤU GIÁ VẬT PHẨM ERC-721 VÀ ERC-1155 TRÊN NỀN TẢNG ETHEREUM

Giảng viên hướng dẫn: ThS. Nguyễn Tấn Toàn

Sinh viên thực hiện: Nguyễn Đức Hướng 19521592

Ngô Dương Kha 19520117

TP HCM, 06/2022

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

……, ngày ……tháng …… năm 2022

Người nhận xét

(Ký tên và ghi rõ họ tên)

LỜI MỞ ĐẦU

NFT là viết tắt của cụm từ Non-fungible token, tạm dịch là tài chứng không thể đổi ngang, loại tài chứng này dựa trên công nghệ blockchain và thường đại diện cho các tác phẩm, sản phẩm dễ bị sao chép như hình ảnh, video, âm thanh và các tệp kỹ thuật số. Không giống với các vật thể số có thể tái sản xuất vô hạn khác, mỗi NFT có chữ kí số riêng biệt, đánh dấu tính độc nhất của nó. Chúng thường được giao dịch trên mạng blockchain bằng các đồng tiền mã hoá hoặc bằng đồng USD. Mặc dù ai cũng có thể xem các tài sản NFT, nhưng chỉ người tạo ra hoặc người mua mới có quyền sở hữu chính thức.

Nhờ những tính chất độc đáo mà NFT được ứng dụng rất đa dạng vào nhiều lĩnh vực, nổi bật hiện nay như là tác phẩm nghệ thuật (âm nhạc, hội họa, phim ảnh), trò chơi diện tử (vật phẩm game), thể thao (pack vật phẩm)…

NFT được giao dịch từ khoảng năm 2017. Nó bắt đầu thu hút chú ý từ đầu năm 2021 trước khi bùng nổ vào khoảng tháng 8/2021. Theo số liệu thống kê, khối lượng giao dịch của thị trường NFT đạt ít nhất 44,2 tỷ USD trong năm 2021, trong khi con số của năm 2020 chỉ khoảng 106,5 triệu USD và 15,2 triệu USD của năm 2019. Bên cạnh đó, Việt Nam cũng lọt vào top những nước có lượng người dùng NFT nhiều nhất trên thế giới con số 2,19 triệu người trong năm 2021.

Cùng với sự phát triển của thị trường giao dịch NFT, nhu cầu sử dụng một sàn giao dịch chuyên dụng dành cho NFT cũng rất được quan tâm, nhiều sàn giao dịch lớn đã ra đời để phục vụ nhu cầu mua và bán các tài sản kỹ thuật số.

Nắm bắt được nhu cầu này, em đã quyết định tìm hiểu công nghệ blockchain để xây dựng hệ thống đấu giá vật phẩm NFT trên nên tảng Ethereum.

LỜI CẢM ƠN

Đầu tiên, nhóm xin gửi lời cảm ơn chân thành đến tập thể quý Thầy Cô Trường Đại học Công nghệ thông tin – Đại học Quốc gia TP.HCM và quý Thầy Cô khoa Công nghệ phần mềm đã giúp cho em có những kiến thức cơ bản làm nền tảng để thực hiện đề tài này.

Đặc biệt, em xin gửi lời cảm ơn và lòng biết ơn sâu sắc nhất tới thầy Nguyễn Tấn Toàn. Thầy đã trực tiếp hướng dẫn tận tình, sửa chữa và đóng góp nhiều ý kiến quý báu giúp em hoàn thành tốt báo cáo môn học của mình. Trong thời gian một học kỳ thực hiện đề tài, em đã vận dụng những kiến thức nền tảng đã tích lũy đồng thời kết hợp với việc học hỏi và nghiên cứu những kiến thức mới. Từ đó, em vận dụng tối đa những gì đã thu thập được để hoàn thành một báo cáo đồ án tốt nhất. Tuy nhiên, trong quá trình thực hiện, em không tránh khỏi những thiếu sót. Chính vì vậy, em rất mong nhận được những sự góp ý từ phía Thầy nhằm hoàn thiện những kiến thức mà em đã học tập và là hành trang kiến thức giúp em phát triển trong tương lai.

Sau cùng, nhóm xin kính chúc Thầy thật dồi dào sức khỏe, niềm tin để tiếp tục thực hiện sứ mệnh cao đẹp của mình là truyền đạt kiến thức cho thế hệ mai sau.

Xin chân thành cảm ơn các quý Thầy Cô!

Nhóm sinh viên thực hiện

MỤC LỤC

DANH MỤC BẢNG

DANH MỤC ẢNH

Chương 1 TỔNG QUAN

1.1. Tên đề tài

"Nghiên cứu và xây dựng hệ thống đấu giá vật phẩm ERC-721 và ERC-1155 trên nền nảng Ethereum".

1.2. Giới thiệu đề tài

Thị trường NFT ngày càng trở nên hấp dẫn cùng với sự phát triển của công nghệ và sự phổ biến của khái niệm Metaverse (Vũ trụ ảo). Công ty Meta (Facebook) đã có đoạn video giới thiệu về Metaverse, trong đó nhắc đến NFT như một phần quan trọng của việc xây dựng vũ trụ ảo.

Cùng với sự phát triển của thị trường giao dịch NFT, nhu cầu sử dụng một sàn giao dịch chuyên dụng dành cho NFT cũng rất được quan tâm, nhiều sàn giao dịch lớn đã ra đời để phục vụ nhu cầu mua bán các tài sản kỹ thuật số và giải quyết những vấn đề liên quan.

Tính minh bạch: Giao dịch mua bán cần minh bạch. Minh bạch là điều tất yếu không thế thiếu của cuộc sống, đặc biệt là trong những giao dịch liên quan tới tiền và tài sản. Thông qua hệ thống sàn giao dịch, có thể dễ dàng truy xuất nguồn gốc của các tài sản số.

Niềm tin: Đặc thù của các giao dịch NFT là được thực hiện trên không gian mạng blockchain nơi mọi thứ gần như là ẩn danh, vì vậy nên cần có một hệ thống chịu trách nhiệm trung gian đảm bảo cho các giao dịch đó, và các sàn giao dịch NFT với hệ thống giao dịch được xây dựng dựa trên Smart Contract chính là giải pháp cho vấn đề này.

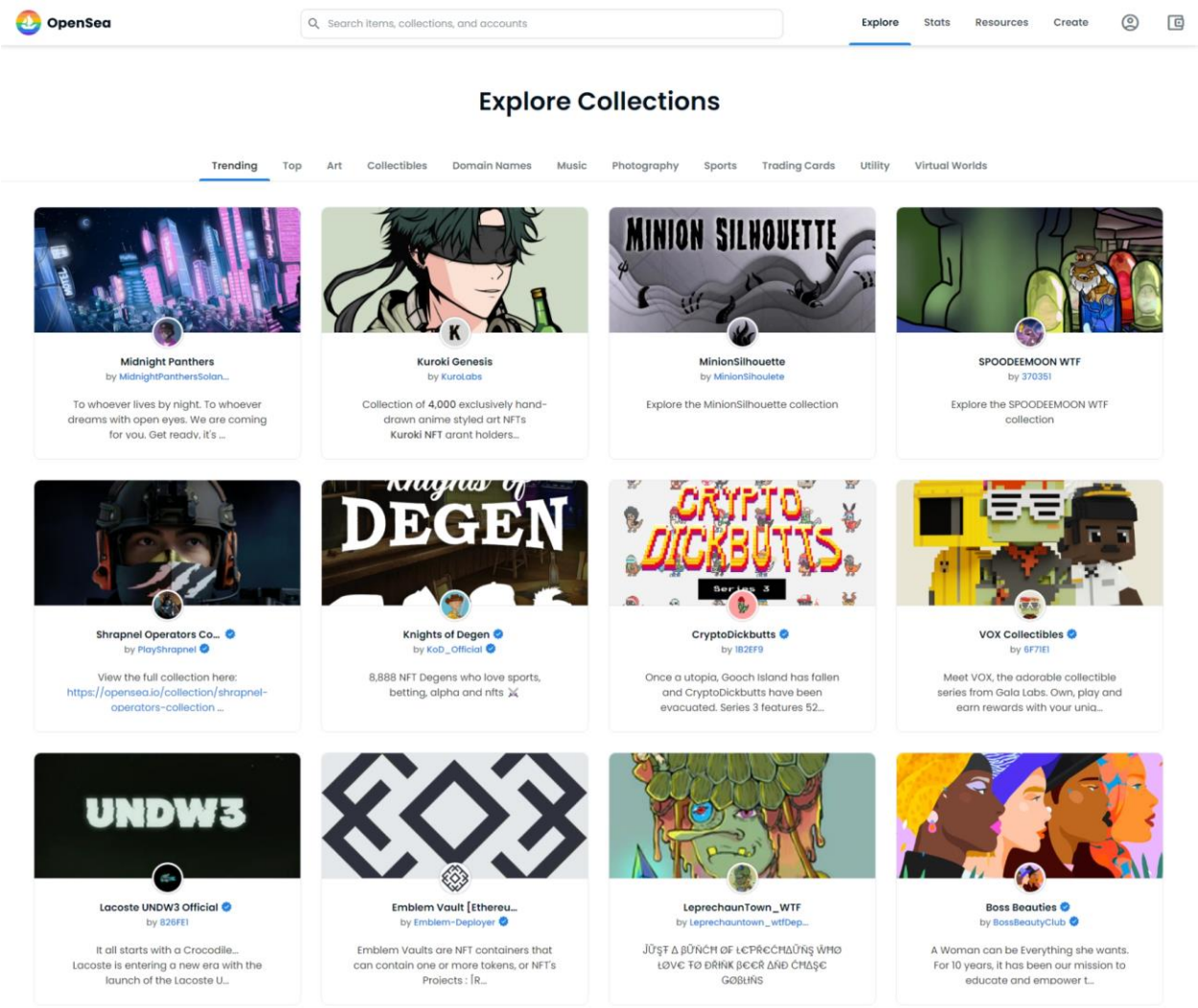
An toàn, nhanh chóng: Các giao dịch được thực hiện bằng Smart Contract một cách chính xác, minh bạch, an toàn và nhanh chóng.

Công nghệ Blockchain và Smart Contract sẽ giúp xây dựng một hệ thống kết nối giữa người bán và người mua mà không cần qua bên thứ ba, từ đó giảm thiểu chi phí cũng như đảm bảo được tính minh bạch, an toàn trong giao dịch.

1.3. Khảo sát hiện trạng

- Các sàn giao dịch NFT nổi tiếng hiện nay:

1.3.1. OpenSea



Ảnh 1-1 Website sàn giao dịch OpenSea

OpenSea được biết đến là sàn giao dịch các vật phẩm kỹ thuật số NFTs (NFTs Marketplace) hoàn toàn phi tập trung đầu tiên và lớn nhất trên toàn cầu. Trong đó, nền tảng cho phép người dùng tạo lập tài khoản để mua bán, trao đổi và giao dịch những vật phẩm sưu tầm (Collections), trò chơi trong game (Game NFT) hoặc những sản phẩm Blockchain dựa trên hoạt động của Smart Contract mà không bị kiểm soát.

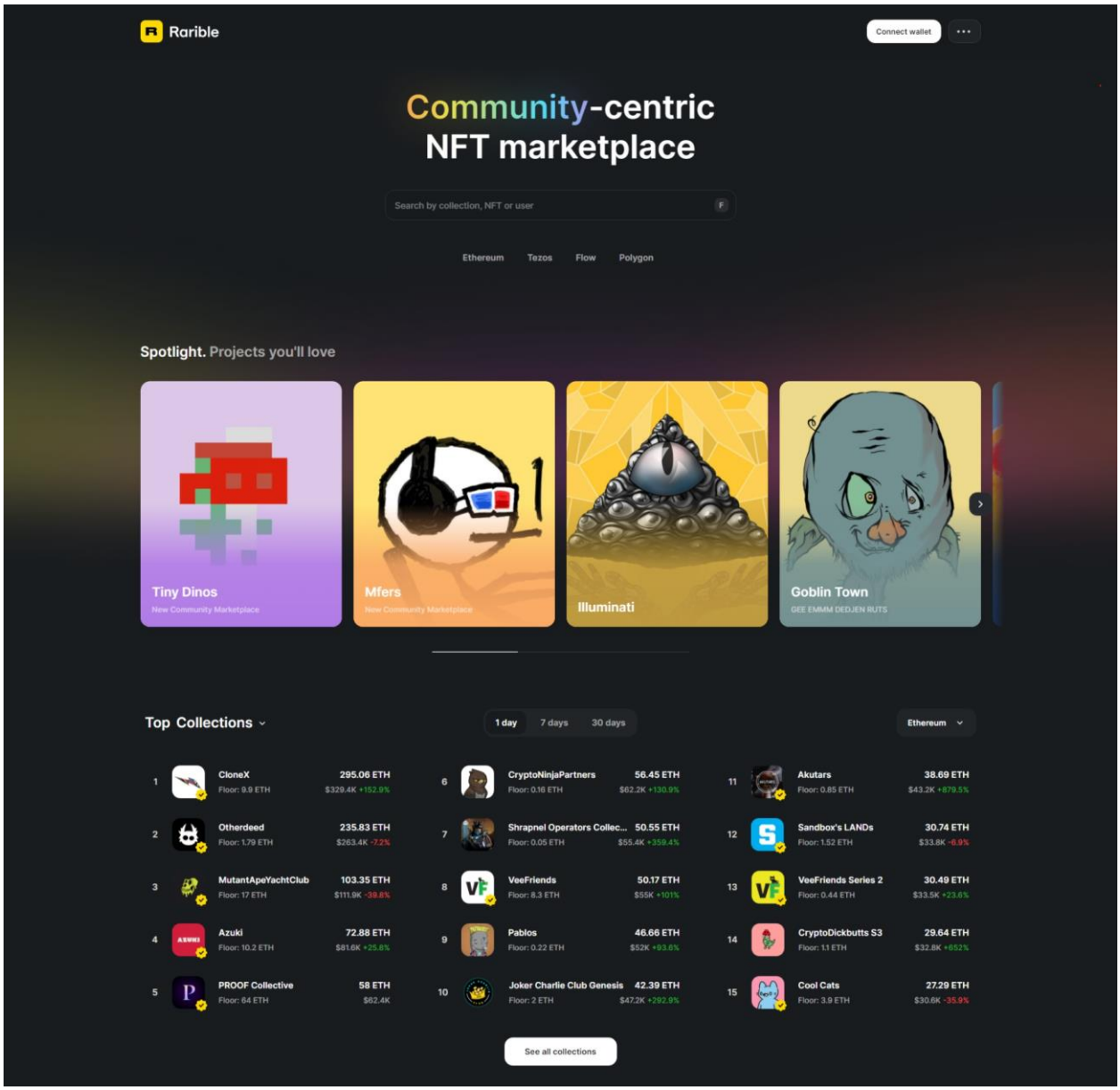
Hàng loạt các nghệ sĩ lớn trên thế giới như Lupe Fiasco, Kevin Kelly và gần đây nhất là rapper Binz cũng đã cho ra mắt bộ sưu tập NFT “Don’t break my heart” dưới nền tảng Tuniver.

Ưu điểm của OpenSea:

- Những giao dịch trên OpenSea đều được xử lý nhanh chóng, minh bạch dưới dạng hợp đồng thông minh (Smart Contract) mà không phải thông qua bất kỳ đơn vị trung gian nào.

- Tính năng bảo mật tốt, hạn chế các vấn đề rủi ro xảy đến bởi các tài sản của người tham gia sẽ được lưu trữ trực tiếp trên ví của họ.
- Người dùng có toàn quyền sở hữu các NFTs mà mình đã mua trên OpenSea.
- Khơi nguồn cảm hứng, thoải mái sáng tạo và các NFTs được công nhận thông qua những phiên đấu giá trên sàn.
- Giao dịch tự do, không bị ràng buộc với mức phí hợp lý.

1.3.2. Rarible



Ảnh 1-2 Website sàn giao dịch Rarible

Rarible (RARI) được biết đến là một thị trường NFT phi tập trung, cho phép người dùng có thể tạo lập và mua bán những bộ sưu tập kĩ thuật số mà không cần nhiều kiến thức

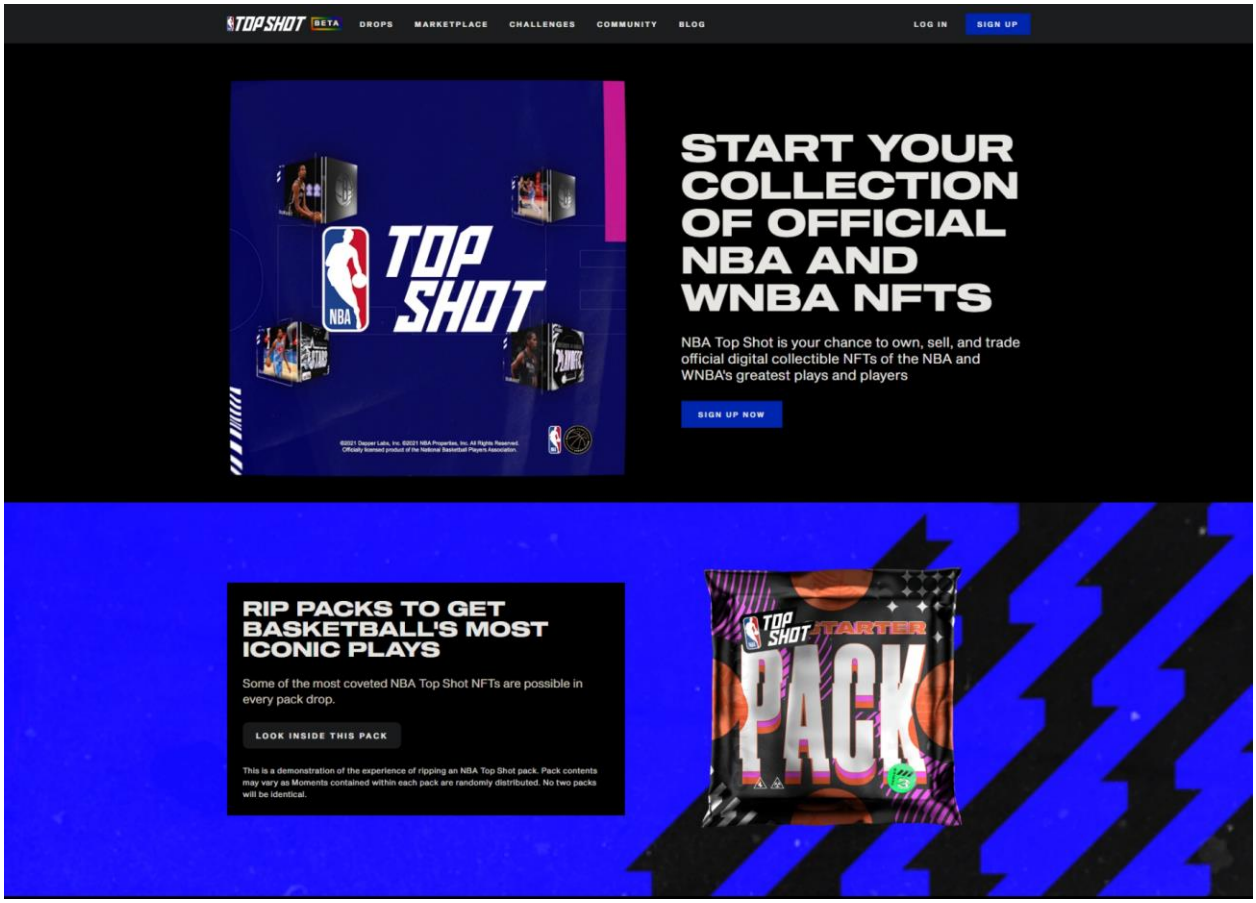
về tiền mã hóa. Toàn bộ tài sản này sẽ được Rarible bảo mật tuyệt đối bằng công nghệ Blockchain.

Tầm nhìn mà Rarible hướng đến không đơn thuần là một nền tảng phi tập trung để bảo mật các tác phẩm nghệ thuật và bộ sưu tập kĩ thuật số của người dùng bằng Blockchain. Rarible còn có tham vọng xây dựng một thị trường giao dịch mà tại đó, người dùng có thể đúc các NFT trên Rarible và họ sẽ được ưu tiên những lợi ích tuyệt vời.

Ưu điểm của Rarible:

- Thị trường mã nguồn mở và không giám sát.
- Tạo điều kiện cho người dùng tạo và đúc mã thông báo kỹ thuật số của riêng họ.
- Trải nghiệm thân thiện với người dùng cho những người không phải lập trình viên.
- Giao dịch ngang hàng với chi phí thấp của NFT hoặc đồ sưu tầm.

1.3.3. NBA Top Shot



Ảnh 1-3 Website sàn giao dịch NBA Top Shot

NBA Top Shot là một loạt các thẻ giao dịch thu thập được phát hành dưới dạng mã thông báo không thể thay thế hoặc NFT. Mỗi NFT đại diện cho một “khoảnh khắc” trong lịch sử bóng rổ dưới dạng một video clip ngắn.

Về cơ bản, NBA Top Shot là ví dụ chính thống về thẻ thu kỹ thuật số. Thay vì được in trên thẻ, chúng sẽ được lưu giữ trên Blockchain. Bạn có thể giữ chúng trong ví kỹ thuật số của mình, gửi chúng cho người khác hoặc rao bán trên các thị trường trực tuyến.

1.4. Mục tiêu hướng đến

Tìm hiểu và nắm vững cơ chế hoạt động của Blockchain, NFT và áp dụng SmartContract vào hệ thống sản giao dịch NFT.

Tìm hiểu về Hardhat Development Enviroment và OpenZeppelin xây dựng SmartContract, liên kết SmartContract với hệ thống.

Tìm hiểu về Ethers.js và ứng dụng trong giao tiếp giữa giao diện người dùng với SmartContract để thực hiện ghi dữ liệu vào Blockchain.

Tìm hiểu lưu trữ phân tán hình ảnh IPFS và ứng dụng vào hệ thống nhằm lưu trữ hình ảnh phân tán, giúp dữ liệu không bao giờ được thay đổi.

Tìm hiểu về library ReactJS và framework Next.js để xây dựng phần giao diện người dùng vì mang nó lại sự trải nghiệm tốt, khả năng chịu tải cao và mạnh mẽ trong việc quản lý state, thread và bất đồng bộ.

Xây dựng hệ thống sàn giao dịch NFT đảm bảo các tính minh bạch, an toàn, nhanh chóng và tiện lợi.

Chương 2 CƠ SỞ LÝ THUYẾT

2.1. Blockchain

2.1.1. Giới thiệu

Blockchain, tên ban đầu là block chain, là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian, 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.

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.**

"Blockchain là một sổ cái kỹ thuật số (ledger) không thể bị phá hỏng của các giao dịch kinh tế, có thể được lập trình để ghi lại không chỉ những giao dịch tài chính mà có thể ghi lại tất cả mọi thứ có giá trị" - Don & Alex Tapscott, Blockchain Revolution (2016).

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 và được lưu trữ trên nhiều máy tính trải rộng trên mạng. Các máy tính riêng lẻ này được gọi là các nút (node).

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.

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

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

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

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

2.1.2. Tính chất của blockchain

Tăng hiệu suất làm việc của hệ thống: đây là tính năng đầu tiền và cốt yếu nhất của phần mềm này. Điều tuyệt vời nhất của Blockchain đó chính là nó có thể gia tăng công suất hoạt động của toàn bộ hệ thống. Nhờ vào việc sẽ có nhiều máy tính hoạt động cùng một lúc trong cùng một mạng lưới, giúp giải quyết công việc hiệu quả hơn - tối ưu hơn so với việc chỉ tập trung quyền kiểm soát vào một máy tính cụ thể.

Tính năng bảo mật tốt hơn: công nghệ Blockchain sẽ có tính năng bảo mật tốt hơn bởi vì sẽ không có bất kỳ một khe hở nào có thể được tận dụng để đánh sập hệ thống - thậm chí là đối với các hệ thống tài chính có nguy cơ tiềm ẩn cao nhất.

Tính ổn định: tạo dựng một nền tảng sổ cái (ledgers) ổn định là mục tiêu cốt lõi của Blockchain. Bất kỳ nền tảng tập trung nào đều cũng có thể dễ dàng bị xâm nhập bởi các hacker và đòi hỏi sự tin tưởng từ bên thứ ba. Tuy nhiên, hệ thống Blockchain như Bitcoin luôn giữ cho dữ liệu sổ cái của mình trong trạng thái luôn được chuyển tiếp ổn định. Chúng ta sẽ luôn cần đạt được sự đồng thuận giữa các miners (người dùng Bitcoin), exchange

(giao dịch) và nodes operator (nút toán tử) trong Bitcoin để có thể thay đổi được dữ liệu của Blockchain.

Xử lý nhanh hơn: hệ thống ngân hàng truyền thống sẽ mất rất nhiều ngày để có thể xử lý được các dữ liệu. Điều này dẫn đến lý do vì sao các ngân hàng luôn cần phải cập nhật lại hệ thống của mình thường xuyên. Tuy nhiên, Blockchain hoàn toàn có thể xử lý được vấn đề này bởi vì chúng xử lý dữ liệu với một tốc độ rất nhanh. Ưu điểm này đã giúp rất nhiều ngân hàng tiết kiệm được rất nhiều thời gian, tiền bạc và mang lại sự tiện lợi cho các khách hàng của mình.

Nền tảng phi tập trung: công nghệ phi tập trung cung cấp cho bạn khả năng lưu trữ tài sản vào trong hệ thống thông qua Internet. Chủ sở hữu có quyền kiểm soát trực tiếp hệ thống và chuyển giao tài sản của mình sang bất kỳ một người nào khác thông qua một chiếc chìa khóa riêng (chìa khóa ảo). Công nghệ Blockchain đã và đang chứng minh được khả năng của mình trong công cuộc phi tập trung hóa các trang web và sở hữu sức mạnh đem lại thay đổi to lớn cho tất cả các nền công nghiệp.

Tính khắc phục: thông qua công nghệ của Blockchain, chúng ta sẽ có thể giải quyết được những vấn đề rắc rối liên quan đến việc gian lận. Đặc biệt, những quốc gia - nơi mà sự tin tưởng của người dùng đối với các tính năng công nghệ vẫn còn thấp - sẽ là "vùng đất hy vọng" cho sự phát triển của phần mềm Blockchain. Gần đây, có rất nhiều phương pháp mới cũng đã được giới thiệu như là phương tiện chứng minh một người tham dự vào công việc tính toán và vai trò của người miner đó chính là xây dựng các khối thông tin.

2.1.3. Ứng dụng của blockchain

Blockchain là xu hướng công nghiệp hiện nay và được ứng dụng trong nhiều lĩnh vực, ngành nghề khác nhau. Những quốc gia hoặc doanh nghiệp lớn đều dành nhiều công sức và tài chính để nghiên cứu công nghệ Blockchain với mong muốn tạo ra những sản phẩm thực tiễn và bảo mật cao.

- Ứng dụng công nghệ Blockchain trong sản xuất:
    - Quản lý các kho bãi sản xuất, hàng tồn kho.
    - Kiểm soát nguồn cung nguyên liệu trong chuỗi cung ứng.

- Theo dõi số lượng hàng mua vào và bán ra, kiểm tra quy trình sản xuất.
- Truy xuất nguồn gốc hàng hòa, sản phẩm.

- Ứng dụng công nghệ Blockchain trong lĩnh vực chăm sóc sức khỏe, y tế:
  - Liên kết và phát triển ứng quản lý chất lượng và quản lý bệnh lý.
  - Kiểm soát chuỗi cung ứng thuốc và vật tư y tế.
  - Đảm bảo tính minh bạch và khả năng tự động hóa đối với giao dịch khám chữa bệnh, quyền sở hữu dữ liệu tình trạng sức khỏe của người bệnh, kết quả xét nghiệm lâm sàng.
- Ứng dụng công nghệ Blockchain trong ngành giáo dục:
  - Theo dõi và lưu trữ dữ liệu học tập của học sinh, sinh viên.
  - Đánh giá mức độ phù hợp của ứng viên trong quá trình đào tạo, từ đó sẽ có những điều chỉnh hợp lý.
  - Đánh giá năng lực của cá nhân so với yêu cầu đầu vào dựa trên dữ liệu học vấn đã được ghi lại.
  - Quản lý mức độ đánh giá sự uy tín trong các bài nghiên cứu khoa học.
- Ứng dụng công nghệ Blockchain trong lĩnh vực nông nghiệp:
  - Quản lý chuỗi cung cấp của sản phẩm, hàng tồn kho.
  - Lưu trữ thông tin của hàng hóa, quy trình chăm sóc, tiêu chuẩn cho thực phẩm.
  - Truy xuất nguồn gốc và vòng đời sản xuất nông sản.
- Ứng dụng công nghệ Blockchain trong lĩnh vực tài chính - ngân hàng:
  - Xác thực thông tin khách hàng, khả năng tín dụng trực tiếp mà không cần qua trung gian.
  - Tính bảo mật cao và tiện lợi với các công nghệ xác minh danh tính, thanh toán nhan chóng và cập nhật giao dịch liên tục.
  - Quản lý và hạn chế rủi ro về trục trặc kỹ thuật và vỡ nợ trước khi thực hiện giao dịch.

- Hệ thống quản lý thông minh cho phép các tính năng liên tục đổi mới và cải tiến dựa trên sự chấp thuận của tất cả người dùng trong chuỗi.

- Ứng dụng công nghệ Blockchain trong ngành bán lẻ:
  - Quản lý hàng hóa thông qua mã định danh trên hệ thống.
  - Đảm bảo chất lượng hàng hóa khi có giao dịch giữa nhà sản xuất và công ty vận tải.
  - Quản lý lưu thông của dòng tiền phát sinh từ giao dịch giúp hạn chế thiệt hại và xử lý ngay những vấn đề phát sinh nếu có.

Bên cạnh đó ứng dụng của Blockchain còn xuất hiện trong nhiều lĩnh vực khác như thương mại điện tử, an ninh mạng, bất động sản,… Sự phổ biến của công nghệ Blockchain là rất lớn, với những tín hiệu thực tế hiện nay rất có thể công nghệ này sẽ đi vào từng ngóc ngách của đời sống con người.

2.2. Smart Contract

2.2.1. Giới thiệu

Smart Contract (Hợp đồng thông minh) là các chương trình chạy trên Blockchain. Hợp đồng thông minh cũng giống như một hợp đồng kỹ thuật số bị bắt buộc thực hiện bởi một bộ quy tắc cụ thể. Các quy tắc này do bộ mã mát tính xác định trước mà tất cả các nút (node) trong mạng đều phải sao chép và thực thi các quy tắc đó.

Về bản chất, Smart Contract chỉ là một đoạn mã chạy trên Blockchain, cho phép tạo ra các giao thức Permissionless (không cần cấp quyền), có nghĩa là:

- Hai bên trong hợp đồng có thể đưa ra các cam kết thông qua Blockchain mà không cần phải biết về danh tính hay 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.

Mỗi Blockchain có một phương pháp triển khai hợp đồng thông minh khác nhau, trong đó nổi bật nhất vẫn là Smart Contract chạy trên máy ảo của Ethereum (EVM).

2.2.2. Cơ chế hoạt động Smart Contract

Smart Contract hoạt động như một chương trình tất định, các Smart Contract sẽ thực thi một tác vụ cụ thể trong trường hợp thỏa mãn các điều kiện nhất định. Do đó, một hệ thống Smart Contract thường tuân theo các câu lệnh "if...then...".

Đầu tiên, các điều khoản trong hợp đồng sẽ được viết bằng ngôn ngữ lập trình, sau đó được mã hóa và chuyển vào một block trong Blockchain. Sau khi chuyển vào block, Smart Contract này sẽ được phân phối và sao chép lại bởi các node đang hoạt động trên nền tảng đó. Sau khi có nhận lệnh triển khai thì hợp đồng sẽ được triển khai theo đúng như điều khoản định sẵn. Đồng thời, Smart Contract cũng sẽ tự động kiểm tra quá trình thực hiện những cam kết, điều khoản được nêu trong hợp đồng.

Trên Ethereum, các Smart Contract chịu trách nhiệm thực thi và quản lý các hoạt động diễn ra trên Blockchain khi những người dùng (address) tương tác với nhau. Bất kỳ địa chỉ nào không phải là Smart Contract đều được gọi là Tài khoản độc lập (EOA). Do đó, Smart Contract sẽ do máy tính kiểm soát và EOA do người dùng kiểm soát.

Smart Contract được triển khai thông qua giao dịch Blockchain và chúng chỉ được kích hoạt khi một EOA hoặc các Smart Contract khác call chúng. Tuy nhiên, kích hoạt đầu tiên luôn từ phía người dùng.

2.2.3. Tính chất của Smart Contract

Phân tán: được sao chép và phân phối trong tất cả các node của mạng Ethereum. Đây là một điểm khác biệt so với các giải pháp khác dựa trên các máy chủ tập trung.

Tất định: 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 thay đổi dù người thực hiện là ai.

Tự động: có thể tự động hóa tất cả các loại tác vụ, nó hoạt động như một chương trình tự thực hiện. Tuy nhiên, trong hầu hết các trường hợp, nếu Smart Contract không được kích hoạt, nó sẽ duy trì trạng thái "không hoạt động" và sẽ không thực hiện bất kì hành động nào.

Không thể sửa đổi: không thể sửa đổi Smart Contract sau khi triển khai. Chỉ có thể "xóa" chúng nếu chức năng này đã được thêm vào từ trước.

Có thể tùy chỉnh: 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.

Không cần dựa trên sự tin cậy: 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.

Minh bạch: vì các Smart Contract dựa trên một Blockchain public, không ai có thể thay đổi mã nguồn của chúng, mặc dù bất kỳ ai cũng có thể xem được.

2.3. Nền tảng Ethereum

2.3.1. Giới thiệu

Ethereum hoạt động trên cơ sở mạng Blockchain và được cấu thành bởi các máy tính hay còn gọi là node. Để tham gia vào mạng lưới, các node cần cài đặt phần mềm Ethereum Client – đồng nghĩa với việc các node sẽ phải chạy chương trình máy ảo EVM để thực thi các Smart Contract.

Khi các nhà phát triển muốn xây dựng ứng dụng phi tập trung (dapps) trên Ethereum, họ cần phải triển khai các Smart Contract thông qua ngôn ngữ lập trình Solidity. Và để kích hoạt việc thực thi các Smart Contract, mạng lưới cần đến một lượng phí gọi là "gas". Phí gas trong mạng Ethereum sẽ được thanh toán bằng Ether (ETH).

Khi giao dịch được thực thi, đây là lúc cần đến việc xác nhận giao dịch đó có hợp lệ hay không. Trong mạng Ethereum thành phần đảm nhiệm việc xác nhận giao dịch này là Miner Node. Để mạng lưới vận hành độc lập, nhất quán thì các Miner Node phải tuân theo luật đồng thuận là Consensus (cơ chế đồng thuận). Ethereum sử dụng Consensus tên là Proof of Work (PoW) – các Miner Node phải chứng minh được công việc họ đã hoàn thành và thông báo đến toàn mạng lưới. Sau đó, các Miner Node khác trong mạng lưới sẽ xác nhận xem bằng chứng này là có hợp lệ hay không. Khi bằng chứng được thông qua, dữ liệu giao dịch sẽ được ghi vào Blockchain của Ethereum và không thể thay đổi.

2.3.2. Các thành phần trong

Ethereum

Tài khoản: trạng thái của Ethereum bao gồm nhiều đối tượng nhỏ (các tài khoản trực tuyến) có thể tương tác với nhau thông qua cơ chế truyền message. Bất kỳ tài khoản nào cũng có một định danh duy nhất (address) là 160 bit. Ethereum có 2 loại tài khoản:

- Tài khoản người dùng (EOA) được quản lý bởi private key và không có chứa mã nguồn.
- Tài khoản hợp đồng chứa mã nguồn và được quản lý bởi mã nguồn trong hợp đồng, tài khoản hợp đồng chỉ có address mà không có private key như tài khoản người dùng.

Trạng thái của tài khoản: bao gồm 4 thành phần có trong bất kỳ tài khoản nào:

- nonce: thể hiện số lượng giao dịch đã được gửi từ tài khoản nếu tài khoản là tài khoản người dùng, là số lượng hợp đồng được tạo nếu tài khoản là tài khoản hợp đồng.
- balance: số lượng wei tài khoản đang có (1 ETH = 10^{18} wei).
- storageRoot: giá trị băm của phần gốc (root) của cây Merkle Storage. Cây Merkle Storage chứa giá trị băm của các biến có trong Storage của tài khoản và theo mặc định là trống.
- codeHash: giá trị băm của mã hợp đồng ở dạng bytecode trong EVM. Đối với các tài khoản người dùng thì trường codeHash là chuỗi trống.

Trạng thái toàn cục của Ethereum: bao gồm ánh xạ giữa các address và trạng thái tài khoản. Ánh xạ này được lưu trữ trong một cấu trúc dữ liệu được gọi là cây Merkle.

Gas và phí giao dịch: mọi tính toán xảy ra trên mạng Ethereum đều phải trả phí, khoản phí này được trả theo mệnh giá gọi là “gas”. Gas là đơn vị được sử dụng đề đo lường các khoản phí cần thiết cho một tính toán cụ thể. Gas Price là lượng ETH bạn sẵn sàng chi cho mỗi đơn vị gas. Với mỗi giao dịch, người gửi đặt Gas Limit và Gas Price. 2 thông số này thể hiện số lượng gas mà người dùng sẵn sàng chi trả tối đa cho một giao dịch.

Giao dịch: các giao dịch xảy ra giữa các tài khoản khác nhau là lúc trạng thái toàn cục của Ethereum được chuyển từ trạng thái này sang trạng thái khác. Có 2 loại giao dịch là message calls và contract creator. Tất cả các giao dịch có chứa các thành phần sau:

- nonce: số lượng giao dịch đã được gửi bởi người gửi (giao dịch hợp lệ).
- gasPrice: số wei phải trả cho 1 gas.
- gasLimit: số gas tối đa mà người gửi sẵn sàng trả cho giao dịch.
- to: địa chỉ tài khoản nhận giao dịch.
- value: số wei mà tài khoản người gửi gửi cho tài khoản nhận.
- v, r, s: các thông số được tạo ra từ thuật toán ECDSA giúp cho các node trong mạng có thể xác thực chữ ký số của người gửi.
- init (chỉ có trong giao dịch tạo hợp đồng): một đoạn mã EVM được sử dụng để khởi tạo tài khoản hợp đồng mới. init chỉ được chạy 1 lần và sau đó bị loại bỏ.
- data: dữ liệu đầu vào (tham số) của message calls.

Block: tất cả các giao dịch được nhóm lại với nhau thành các block trên mạng. Một Blockchain chứa một chuỗi các block như vậy được nối với nhau. Trong Ethereum, một block bao gồm:

- Block header: bao gồm parentHash, ommersHash, beneficiary, stateRoot, transactionRoot, receipts, logsBloom, difficulty, number, gasLimit, gasUsed, timestamp, extraData, mixHash và nonce.
- Thông tin về tất cả các giao dịch được gom trong block đó
- Các Ommers của nó.

Thực thi giao dịch: tất cả các giao dịch phải đáp ứng một bộ yêu cầu ban đầu để được thực hiện, bao gồm:

- Giao dịch phải định dạng ở chuẩn encode RLP.
- Chữ ký giao dịch là hợp lệ.
- Số nonce trong giao dịch phải bằng số nonce của tài khoản gửi giao dịch.
- gasLimit phải bằng hoặc lớn hơn intrinsic gas (lượng gas mà giao dịch sử dụng trước khi chạy bất cứ đoạn mã nào) được sử dụng trong giao dịch

2.4. NFT – Non-Fungible Token

2.4.1. NFT là gì?

NFT (Non-Fungible Token) là tài sản số hiện diện trên một chuỗi số (Blockchain), Blockchain này có nhiệm vụ như một sổ cái đảm bảo tính xác thực của tài sản lẫn chủ sở hữu. Không giống với các vật thể số có thể tái sản xuất vô hạn khác, mỗi NFT có chữ ký số riêng biệt, đánh dấu tính độc nhất của nó.

Bản thân NFT không phải là một tài sản vật lý, không thể cầm nắm được, mà là một loại mã hóa để lưu trữ và giao dịch trên thế giới số. Nói cách khác, NFT là một "dữ liệu" chứa thông tin nhận dạng và xác minh tài sản được lưu giữ trên Blockchain, mỗi "mã" đại diện cho một tài sản. Vậy nên, khi "mua" một sản phẩm NFT, không có nghĩa là bạn mang sản phẩm đó về đặt để trong nhà, mà bạn đã "mua" bản quyền sở hữu của tác phẩm đó.

2.4.2. Tính chất của NFT

Việc phát minh ra NFT đã và đang được một số nhà đầu tư cho rằng sẽ tạo nhiều cơ hội cho thị trường mua bán các tài sản số có giá trị nhờ những đặc trưng rất riêng của NFT dựa trên công nghệ Blockchain. Những đặc tính nổi bật của NFT bao gồm:

- **Tính không thể phân chia:** khác với Ether hay Bitcoin có thể chia nhỏ. NFT là tài sản nguyên vẹn và không thể phân chia.
- **Tính độc nhất:** mỗi NFT là một sản phẩm duy nhất, không tồn tại sản phẩm tương tự, không thể thay thế và không thể bị sao chép dưới bất cứ hình thức nào.
- **Tính sở hữu:** những tác phẩm nghệ thuật lưu trữ dưới dạng NFT luôn là bản gốc và có thể xác minh quyền sở hữu cũng như tác giả thông qua dữ liệu trên Blockchain.
- **Tính vĩnh cửu:** các NFT có thể tồn tại vĩnh viễn cùng với các thông tin liên quan đến NFT đó.
- **Tính khan hiếm:** mỗi NFT đại diện cho một tệp tin độc nhất vô nhị. Tuy trong thị trường có rất nhiều nhà phát hành NFT nhưng thông thường, ở mỗi bộ sưu tập nhà phát hành sẽ giới hạn số lượng mã thông báo không thể thay thế để gia tăng mức độ khan hiếm của chúng. Đây cũng là một trong những lí do khiến NFT được định giá cao.

2.5. IPFS

2.5.1. Giới thiệu

IPFS (Interplanetary File System) là một hệ thống tập tin phân tán ngang hàng kết nối tất cả các thiệt bị máy tính với nhau. Cụ thể hơn, nó sẽ phân phối dữ liệu được lưu trữ theo hình thức P2P (mạng ngang hàng).

Trong đó, các hoạt động của IPFS chủ yếu dựa vào khả năng tính toán băng thông của tất cả các máy tham gia chứ không tập trung vào một phần nhỏ các máy chủ trung tâm như giao thức HTTP.

Nói cách khác, IPFS là mạng lưới chuyển phát nội dung hoàn toàn phi tập trung cho phép quản lý và lưu trữ dữ liệu một cách linh hoạt. Mỗi máy tính tham gia trong mạng lưới đảm nhận nhiệm vụ download và upload dữ liệu mà không cần sự can thiệp của máy chủ trung tâm.

2.5.2. Đặc điểm nổi bật

Nếu được triển khai đúng, IPFS mang lại tiềm năng lớn nhờ cải thiện được tốc độ truyền tải dữ liệu, tránh sự phụ thuộc vào các máy chủ và tiết kiệm chi phí.

Tránh sự phụ thuộc vào máy chủ:

- Trong các mô hình Client-server như HTTP, khi các máy chủ đang gặp phải sự cố thì chúng sẽ không thể hồi đáp thông tin cho người dùng. Đây cũng là vấn đề lớn nhất mà giao thức HTTP gặp phải khi nó phụ thuộc vào một máy chủ tập trung, điều mà nó không thể cải thiện cũng như khắc phục.
- Với IPFS, nó hoàn toàn bỏ qua khái niệm máy chủ, mà chỉ quan tâm tới nội dung tìm kiếm. Điều này không chỉ giúp chúng ta rút ngắn con đường tới thông tin, mà lại không lo gặp phải các máy chủ kém chất lượng, kém tin cậy.

Mô hình phi tập trung:

- Với một mô hình tập trung, số lượng lớn dữ liệu được tập trung trong tay một số tên tuổi lớn trong lĩnh vực (Facebook, Google, Amazon…) điều này vô tình khiến chúng trở thành tâm điểm cho các hacker tấn công.
- Với mô hình website phân tán (decentralized) của IPFS, các vấn đề này hoàn toàn được khắc phục và không còn chế độ quản lý phân cấp. Các dữ liệu được lưu trữ phân tán và không có một máy chủ tập trung để tấn công, càng nhiều người tham gia vào IPFS thì mạng sẽ càng bảo mật và khó có thể thao túng hơn.

Giảm bớt chi phí: IPFS sẽ cho phép bạn tải dữ liệu lên hoàn toàn về mạng nội bộ dù bạn là ai và đang ở đâu. Do đó loại bỏ sự cần thiết của hàng loạt trạm kết nối và máy chủ Internet, giúp chi phí tổng thể giảm một cách rõ rệt.

2.6. Next.js

Next.js là một framework dùng để phát triển các ứng dụng React theo tư tưởng Isomophic (Universal), được phát triển bởi Zeit. Nhờ Next.js chúng ta có thể dễ dàng tạo được một ứng dụng React theo tư tưởng Isomophic, có bao gồm chức năng Server Side Redering (SSR) và Static Site Generation (SSG).

2.7. Solidity

Solidity là một ngôn ngữ lập trình cấp cao dùng để xây dựng các Smart Contract trên Ethereum. Đối tượng sử dụng của ngôn ngữ này là các nhà lập trình (developer) muốn phát triển các ứng dụng trên Ethereum. Bằng cách sử dụng kết hợp giữa các chữ cái và số, ngôn ngữ lập trình Solidity giúp các developer viết chương trình dễ dàng hơn.

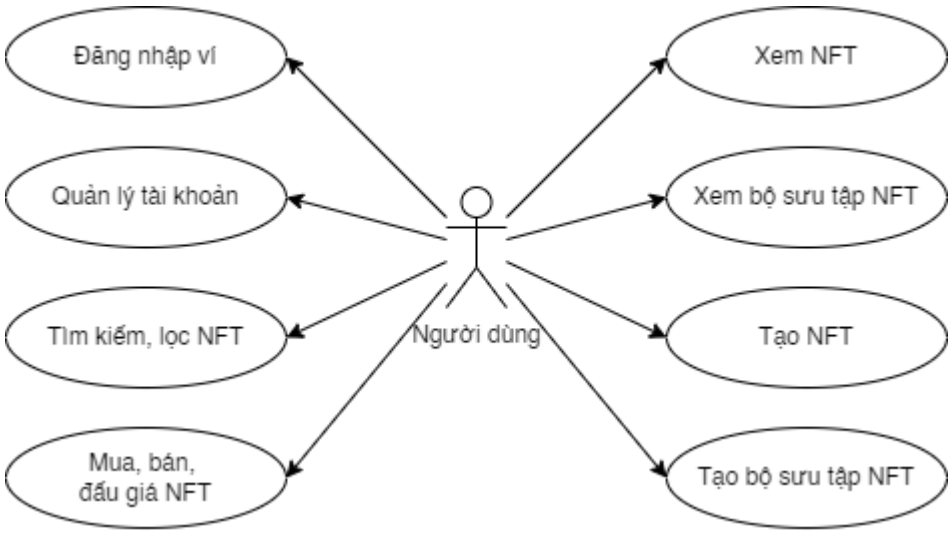
Solidity cho phép nhiều trường hợp sử dụng khác nhau để tạo các Smart Contract trên Ethereum như:

- Mint các Fungible, Non-Fungible token.
- Tạo ra các thị trường cho vay phi tập trung cho các Fungible token.
- Tạo ra các thị trường trao đổi Non-Fungible token.

Sau khi các developer sử dụng Solidity để viết ra các chương trình, một trong những thành phần quan trọng giúp thực thi Solidity code là EVM. Ở cấp độ cao hơn, Solidity cho phép nhà phát triển viết ra các “machine level” code có thể thực thi được trên EVM. Sau đó, trình biên dịch (compiler) được sử dụng để chia nhỏ các dòng code mà các nhà phát triển viết, biến thành các lệnh mà bộ xử lý có thể hiểu và thực thi.

Chương 3 MÔ HÌNH USE-CASE

3.1. Sơ đồ Use-case



Ảnh 3-1 Sơ đồ Use-case tổng quát hệ thống

3.2. Danh sách các Actor

STT	Actor	Ý nghĩa
1	Người dùng	Người chủ sở hữu các NFT. Người chủ sở hữu các bộ sưu tập NFT. Người có nhu cầu bán, đấu giá NFT của mình. Người có nhu cầu mua, đấu giá các NFT đang được đăng trên sàn.

Bảng 3-1 Bảng danh sách các Actor

3.3. Danh sách các Use-case

STT	Tên Use-case	Ý nghĩa
1	Đăng nhập ví	Người dùng đăng nhập vào website thông qua ví Metamask.
2	Quản lý tài khoản	Người dùng có thể thay đổi tên, mô tả, email, ảnh đại diện, ảnh banner của bản thân.
3	Tìm kiếm, lọc NFT	Người dùng tìm kiếm NFT theo tên và có thể lọc theo trạng thái hiện tại của NFT.

4	Mua, bán, đấu giá NFT	Người dùng có thể bán hoặc tạo đấu giá NFT của bản thân. Người dùng có thể mua hoặc đấu giá NFT đang được đăng trên sàn.
5	Xem NFT	Người dùng có thể xem các thông tin của NFT.
6	Xem bộ sưu tập NFT	Người dùng có thể xem các bộ sưu tập NFT hiện có.
7	Tạo NFT	Người dùng có thể tạo mới một NFT thuộc sở hữu của bản thân.
8	Tạo bộ sưu tập NFT	Người dùng có thể tạo mới một bộ sưu tập NFT thuộc sở hữu của bản thân.

Bảng 3-2 Bảng danh sách các Use-case

3.4. Đặc tả Use-case

3.4.1. Đặc tả Use-case "Đăng nhập ví"

Tên chức năng	Đăng nhập ví
Tóm tắt	Đăng nhập vào hệ thống
Dòng sự kiện chính	Hệ thống hiện thỉ màn hình đăng nhập. Người dùng chọn đăng nhập bằng ví Metamask. Hệ thống kiểm tra hợp lệ hay không và thông báo đến người dùng.
Dòng sự kiện khác	Không có.
Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Không có.
Trạng thái hệ thống sau khi thực hiện use-case	Người dùng có thể sử dụng các chức năng cần xác thực.
Điểm mở rộng	Cần mở rộng thêm nhiều ví.

Bảng 3-3 Bảng đặc tả Use-case "Đăng nhập ví"

3.4.2. Đặc tả Use-case "Quản lý tài khoản"

Tên chức năng	Quản lý tài khoản
Tóm tắt	Người dùng xem lại thông tin tài khoản và chỉnh sửa khi cần thiết.
Dòng sự kiện chính	Hệ thống hiện thỉ màn hình thông tin người dùng. Người dùng có thể thay đổi tên, mô tả, email, ảnh đại diện, ảnh banner. Hệ thống kiểm tra hợp lệ hay không và thông báo đến người dùng.
Dòng sự kiện khác	Không có.
Yêu cầu đặc biệt	Người dùng phải là chủ tài khoản.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Đã đăng nhập hệ thống.
Trạng thái hệ thống sau khi thực hiện use-case	Thông tin người dùng được cập nhật.
Điểm mở rộng	Cần mở rộng liên kết đến các mạng xã hội.

Bảng 3-4 Bảng đặc tả Use-case "Quản lý tài khoản"

3.4.3. Đặc tả Use-case "Tìm kiếm, lọc NFT"

Tên chức năng	Tìm kiếm, lọc NFT
Tóm tắt	Người dùng tìm kiếm NFT theo từ khóa và lọc theo các thuộc tính của NFT.
Dòng sự kiện chính	Người dùng nhập từ khóa vào thanh tìm kiếm và lựa chọn các thuộc tính để lọc NFT. Hệ thống sẽ hiển thị những vật phẩm NFT phù hợp với từ khoá tìm kiếm.
Dòng sự kiện khác	Không có.

Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Không có.
Trạng thái hệ thống sau khi thực hiện use-case	Hiển thị danh sách NFT phù hợp với điều kiện đưa ra.
Điểm mở rộng	Cần mở rộng thêm tính năng lọc.

Bảng 3-5 Bảng đặc tả Use-case "Tìm kiếm, lọc NFT"

3.4.4. Đặc tả Use-case "Mua, bán, đấu giá NFT"

Tên chức năng	Mua, bán, đấu giá NFT
Tóm tắt	Người dùng có thể bán và tạo đấu giá những NFT thuộc quyền sở hữu của mình. Người dùng có thể mua và đấu giá những NFT được đăng trên sàn.
Dòng sự kiện chính	Người dùng điền giá bán, giá bắt đầu đấu giá sau đó hệ thống sẽ đăng NFT lên sàn. Người dùng xác nhận mua sau đó hệ thống sẽ chuyển quyền sở hữu NFT cho người dùng. Người dùng nhập số tiền đấu giá sau đó hệ thống sẽ ghi nhận vào lịch sử đấu giá của NFT.
Dòng sự kiện khác	Giá bán, giá bắt đầu đấu giá không hợp lệ hệ thống sẽ gửi lỗi. Giá đấu giá không hợp lệ hệ thống sẽ gửi lỗi.
Yêu cầu đặc biệt	Người dùng là chủ sở hữu NFT mới có thể bán hoặc tạo đấu giá. Người dùng không phải là chủ sở hữu NFT và phải có đủ ETH trong ví để trả tiền mua NFT đó.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Đã đăng nhập hệ thống.

Trạng thái hệ thống sau khi thực hiện use-case	Vật phẩm được đăng lên sàn sau khi bán, tạo đấu giá. Vật phẩm thuộc quyền sở hữu của người dùng sau khi mua. Lưu lịch sử đấu giá khi thực hiện đấu giá.
Điểm mở rộng	Không có.

Bảng 3-6 Bảng đặc tả Use-case "Mua, bán, đấu giá NFT"

3.4.5. Đặc tả Use-case "Xem NFT"

Tên chức năng	Xem NFT
Tóm tắt	Người dùng có thể xem các thông tin của NFT.
Dòng sự kiện chính	Người dùng chọn NFT cần xem và hệ thống sẽ hiển thị thông tin của NFT đó.
Dòng sự kiện khác	Không có.
Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Không có.
Trạng thái hệ thống sau khi thực hiện use-case	Hiển thị thông tin của NFT.
Điểm mở rộng	Không có.

Bảng 3-7 Bảng đặc tả Use-case "Xem NFT"

3.4.6. Đặc tả Use-case "Xem bộ sưu tập NFT"

Tên chức năng	Xem bộ sưu tập NFT
Tóm tắt	Người dùng có thể xem các thông tin của bộ sưu tập NFT.
Dòng sự kiện chính	Người dùng chọn bộ sưu tập NFT cần xem và hệ thống sẽ hiển thị thông tin của bộ sưu tập đó.

Dòng sự kiện khác	Không có.
Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Không có.
Trạng thái hệ thống sau khi thực hiện use-case	Hiển thị thông tin của bộ sưu tập NFT.
Điểm mở rộng	Không có.

Bảng 3-8 Bảng đặc tả Use-case "Xem bộ sưu tập NFT"

3.4.7. Đặc tả Use-case "Tạo NFT"

Tên chức năng	Tạo NFT
Tóm tắt	Người dùng có thể tạo một NFT mới thuộc bộ sưu tập cá nhân.
Dòng sự kiện chính	Người dùng tải lên hình ảnh và nhập thông tin vật phẩm. Hệ thống sẽ kiểm tra thông tin có hợp lệ hay không.
Dòng sự kiện khác	Hệ thống báo lỗi khi thông tin không hợp lệ.
Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Đã đăng nhập hệ thống.
Trạng thái hệ thống sau khi thực hiện use-case	Một NFT được tạo ra trên hệ thống.
Điểm mở rộng	Không có.

Bảng 3-9 Bảng đặc tả Use-case "Tạo NFT"

3.4.8. Đặc tả Use-case "Tạo bộ sưu tập NFT"

Tên chức năng	Tạo bộ sưu tập NFT
Tóm tắt	Người dùng có thể tạo một bộ sư tập NFT mới.
Dòng sự kiện chính	Người dùng tải lên hình ảnh và nhập thông tin vật phẩm. Hệ thống sẽ kiểm tra thông tin có hợp lệ hay không.
Dòng sự kiện khác	Hệ thống báo lỗi khi thông tin không hợp lệ.
Yêu cầu đặc biệt	Không có.
Trạng thái hệ thống trước khi thực hiện use-case	Actor: "Người dùng". Điều kiện: Đã đăng nhập hệ thống.
Trạng thái hệ thống sau khi thực hiện use-case	Một bộ sưu tập NFT được tạo ra trên hệ thống.
Điểm mở rộng	Không có.

Bảng 3-10 Bảng đặc tả Use-case "Tạo bộ sưu tập NFT"

Chương 4 THIẾT KẾ DỮ LIỆU

4.1. Hệ thống Smart Contract

STT	Tên contract	Ý nghĩa
1	NFTMarketplace	Kế thừa từ các contract ERC1155Holder, ERC721Holder, ReentrancyGuard
2	UITToken721	Kế thừa từ các contract ERC721URIStorage, Ownable
3	UITToken1155	Kế thừa từ các contract ERC1155, Ownable
4	VerifySignature	Chứa các phương thức để ký và xác thực user

Bảng 4-1 Bảng hệ thống Smart Contract

4.1.1. Struct "Bid" thuộc NFTMarketplace

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	bidder	address	Địa chỉ người tham gia đấu giá
2	bid	uint256	Số tiền đấu giá
3	bidTime	uint256	Thời gian đấu giá

Bảng 4-2 Bảng dữ liệu Struct "Bid"

4.1.2. Struct "AuctionInfo" thuộc NFTMarketplace

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	startAt	uint256	Thời gian buổi đấu giá bắt đầu
2	endAt	uint256	Thời gian buổi đấu giá kết thúc
3	highestBidder	address	Người đấu giá cao nhất hiện tại
4	highestBid	uint256	Giá trị đấu giá cao nhất hiện tại
5	highestBidTime	uint256	Thời gian tham gia đấu giá cảu người cao nhất

6	startingPrice	uint256	Giá trị khởi đầu của vật phẩm đấu giá

Bảng 4-3 Bảng dữ liệu Struct "AuctionInfo"

4.1.3. Struct "MarketItem" thuộc NFTMarketplace

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	tokenId	uint256	Id của Token
2	nftContract	address	Địa chỉ Collection
3	seller	address	Người bán
4	owner	address	Người sở hữu
5	price	uint256	Giá bán
6	sold	bool	Đã bán
7	bidded	bold	Đã đấu giá
8	isMultiToken	bool	true nếu vật phẩm là ERC1155 / false nếu vật phẩm là ERC721
9	auctionInfo	AutionInfo	Thông tin của phiên đấu giá

Bảng 4-4 Bảng dữ liệu Struct "MarketItem"

4.1.4. Struct "NFTToken" thuộc UITToken721

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	id	uint256	Id của Token
2	uri	String	Uri của Token

Bảng 4-5 Bảng dữ liệu Struct "NFTToken"

4.2. Bảng dữ liệu MongoDB

4.2.1. Schema "Bid"

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	bidder	String	Địa chỉ người đấu giá
2	bid	Number	Số tiền đấu giá
3	bidTime	Date	Thời điểm đấu giá

Bảng 4-6 Bảng Schema "Bid"

4.2.2. Schema "AuctionInfo"

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	startAt	Date	Thời điểm bắt đầu đấu giá
2	endAt	Date	Thời điểm kết thúc đấu giá
3	highestBidder	String	Địa chỉ người đấu giá cao nhất
4	highestBid	Number	Số tiền đấu giá cao nhất
5	highestBidTime	Date	Thời điểm đấu giá cao nhất
6	startingPrice	Number	Số tiền bắt đầu đấu giá
7	bids	Bid[]	Lịch sử đấu giá

Bảng 4-7 Bảng Schema "AuctionInfo"

4.2.3. Schema "Nft"

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	tokenId	Number	Id của token
2	collectionAddress	String	Địa chỉ bộ sưu tập
3	seller	String	Địa chỉ người bán
4	owner	String	Địa chỉ chủ sở hữu
5	name	String	Tên hiển thị

6	description	String	Mô tả
7	image	String	Hình ảnh
8	price	Number	Giá
9	sold	Boolean	Tình trạng bán
10	bidded	Boolean	Tình trạng đấu giá
11	isMultiToken	Boolean	Loại token
12	auctionInfo	AutionInfo	Chi tiết đấu giá

Bảng 4-8 Bảng Schema "Nft"

4.2.4. Schema "User"

STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	username	String	Tên người dùng
2	bio	String	Mô tả
3	email	String	Địa chỉ email
4	wallet	String	Địa chỉ ví Metamask
5	image	String	Hình ảnh
6	banner	String	Hình ảnh bìa
7	refreshToken	String	Mã khôi phục phiên đăng nhập

Bảng 4-9 Bảng Schema "User"

4.2.5. Schema "Collection"

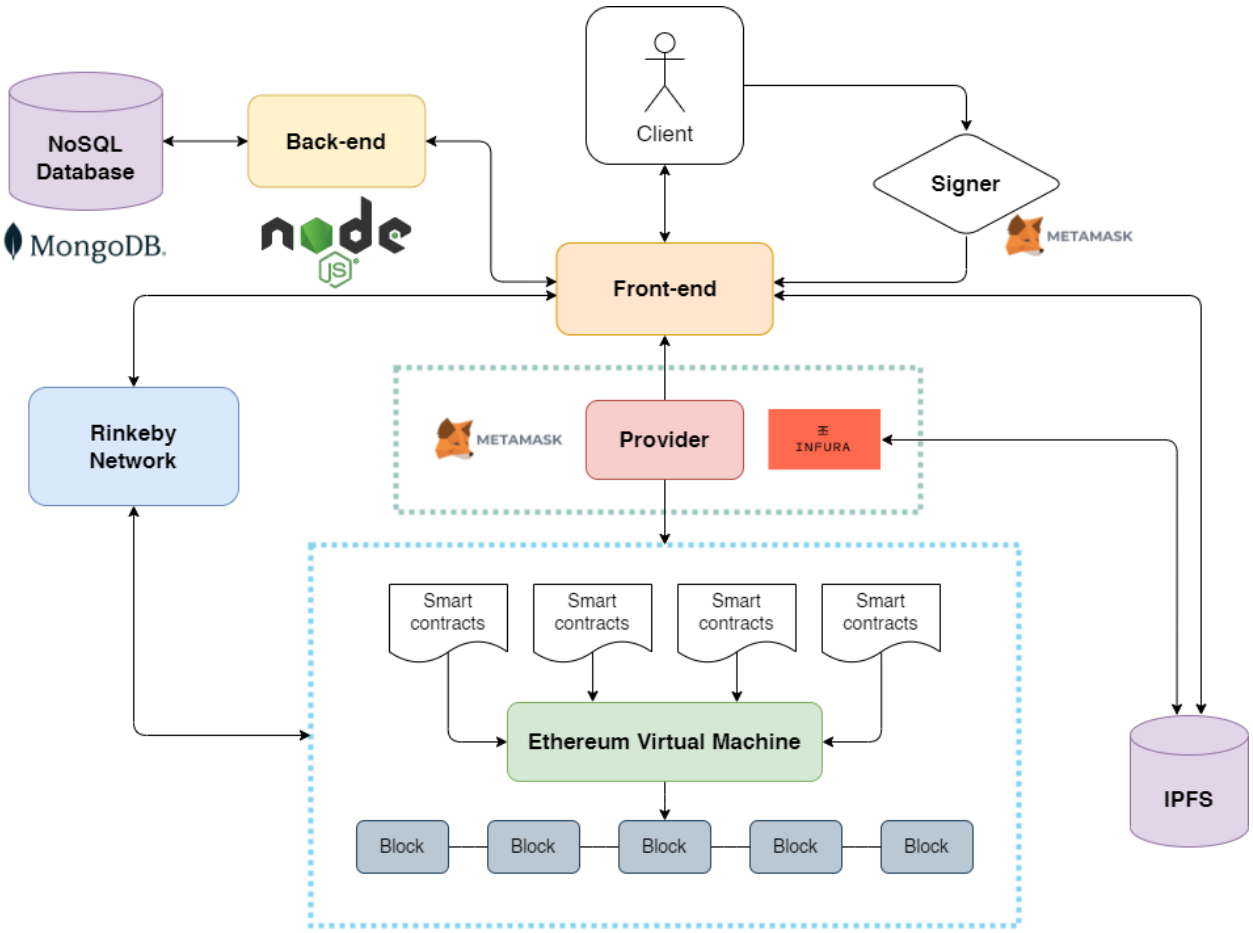
STT	Tên biến	Kiểu dữ liệu	Ý nghĩa
1	name	String	Tên
2	address	String	Địa chỉ
3	description	String	Mô tả

4	image	String	Hình ảnh
5	banner	String	Ảnh bìa
6	isMultiToken	Boolean	Loại token
7	owner	String	Địa chỉ chủ sở hữu

Bảng 4-10 Bảng Schema "Collection"

Chương 5 THIẾT KẾ KIẾN TRÚC

5.1. Kiến trúc hệ thống



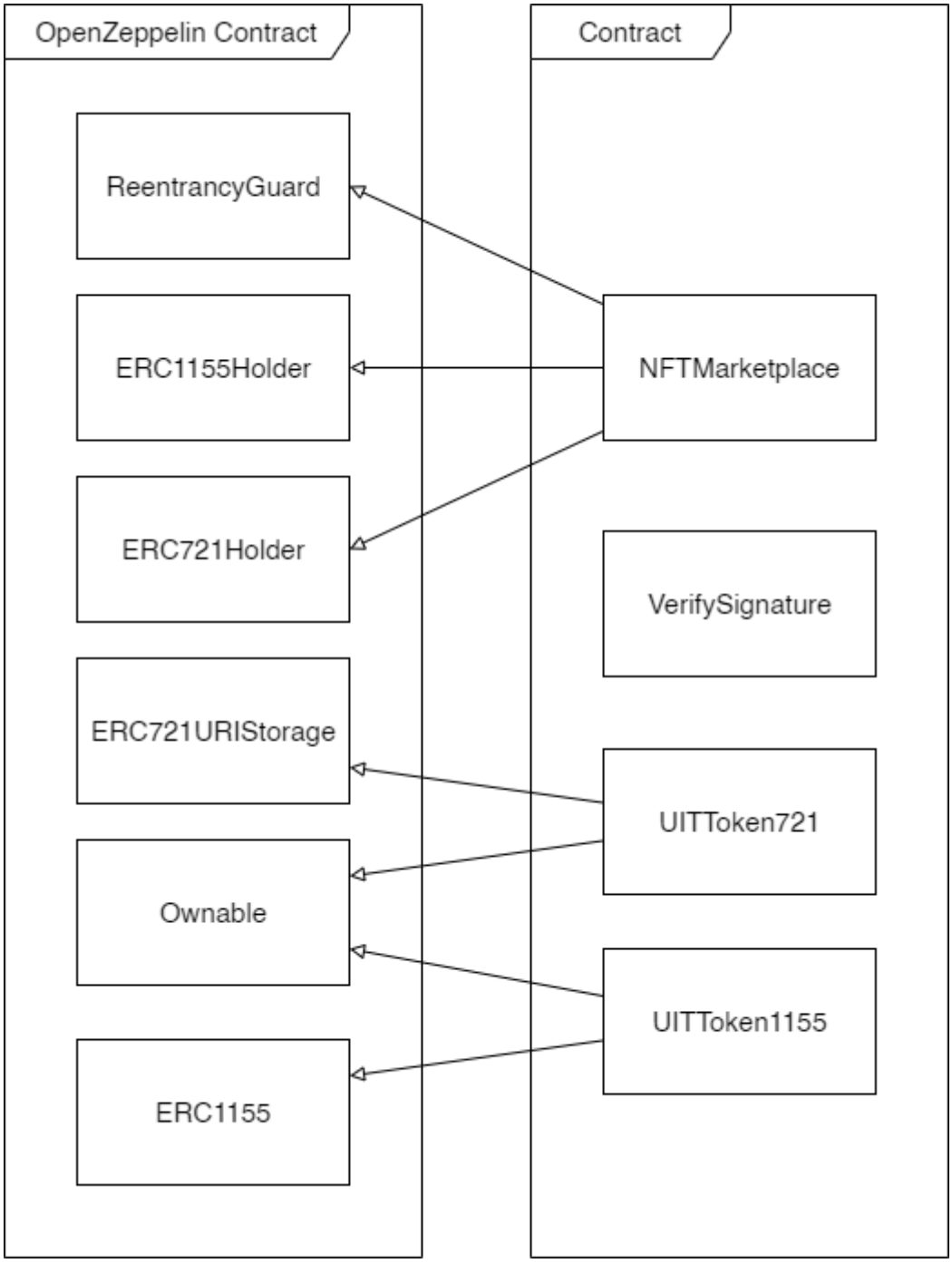
Ảnh 5-1 Kiến trúc tổng quan của hệ thuống

STT	Thành phần	Diễn giải
1	Block	Nơi lưu trữ thông tin giao dịch
2	Ethereum virtual machine	Nơi lưu trữ và thực hiện smart contract
3	Smart contract	Các chương trình chạy trên blockchain
4	Provider	Bên thứ ba giúp tương tác với blockchain
5	IPFS	Mạng lưới chuyển phát nội dung phi tập trung quản lý và lưu trữ file vật lý phân tán
6	Rinkeby network	Phiên bản testnet của Ethereum
7	Front-end	Nơi xây dựng giao diện của trang web

8	Back-end	Cung cấp các API cho phía front-end
9	NoSQL Database	Cơ sở dữ liệu lưu trữ bản sao cơ sở dữ liệu trên
10	Signer	Tìa khoản ví điện tử dùng để xác nhận các giao dịch
11	Client	Người dùng cuối của trang web

Bảng 5-1 Thành phần trong kiến trúc hệ thống

5.2. Kiến trúc Smart Contract



Ảnh 5-2 Kiến trúc Smart Contract

- UITToken721: Contract tạo token chuẩn ERC-721. Gồm các hàm:
  - setParrentApproval(): cho phép contract NFTMarketplace thao tác trên token được tạo từ token này.
  - mintNFT(): hàm đúc NFT.
  - name(), symbol(): lấy giá trị thuộc tính name, symbol của token.

- setName(), setSymbol(): gán giá trị cho thuộc tính name, symbol của token.
- getTokenUri(): lấy giá trị của token uri.
- getTokenIds(): lấy id của token.
- UITToken1155: Contract tạo token chuẩn ERC-1155. Gồm các hàm:
- setParrentApproval(): cho phép contract NFTMarketplace thao tác trên token được tạo từ token này.
- mintNFT(): hàm đúc NFT.
- name(), symbol(): lấy giá trị thuộc tính name, symbol của token.
- setName(), setSymbol(): gán giá trị cho thuộc tính name, symbol của token.
- getTokenUri(): lấy giá trị của token uri.
- getTokenIds(): lấy id của token.

- NFTMarketplace: Contract chính của hệ thống, lưu trữ các xử lý logic của sàn giao dịch
  - createMarketItem(): tạo ra một vật phẩm NFT.
  - listMarketItem(): đưa vật phẩm NFT lên sàn giao dịch bằng phương thức mua trực tiếp.
  - listAuctionItem(): đưa vật phẩm NFT lên sàn giao dịch bằng phương thức đấu giá.
  - createMarketSale(): giúp người dùng mua vật phẩm NFT.
  - cancelListing(): giúp người chủ sở hữu vật phẩm dừng bán vật phẩm NFT.
  - bid(): giúp người dùng tham gia đấu giá vật phẩm NFT.
  - withdrawBid(): giúp người dùng rời khỏi cuộc đấu giá vật phẩm NFT.
  - endAuction(): kết thúc cuộc đấu giá vật phẩm NFT.
- VerifySignature: Contract giúp xác thực người dùng khi giao dịch.
  - getMessageHash(): mã hóa message người dùng gửi đến.

- getEthSignedMessageHash(): chuyển messageHash sang Ethereum Signed Message Hash.
- verify(): xác thực message người dùng gửi tới.
- recoverSigner(): khôi phục địa chỉ người dùng từ Ethereum Signed Message Hash và chữ ký.
- splitSignature(): chia chuỗi chữ ký thành các thông số r, s, v.

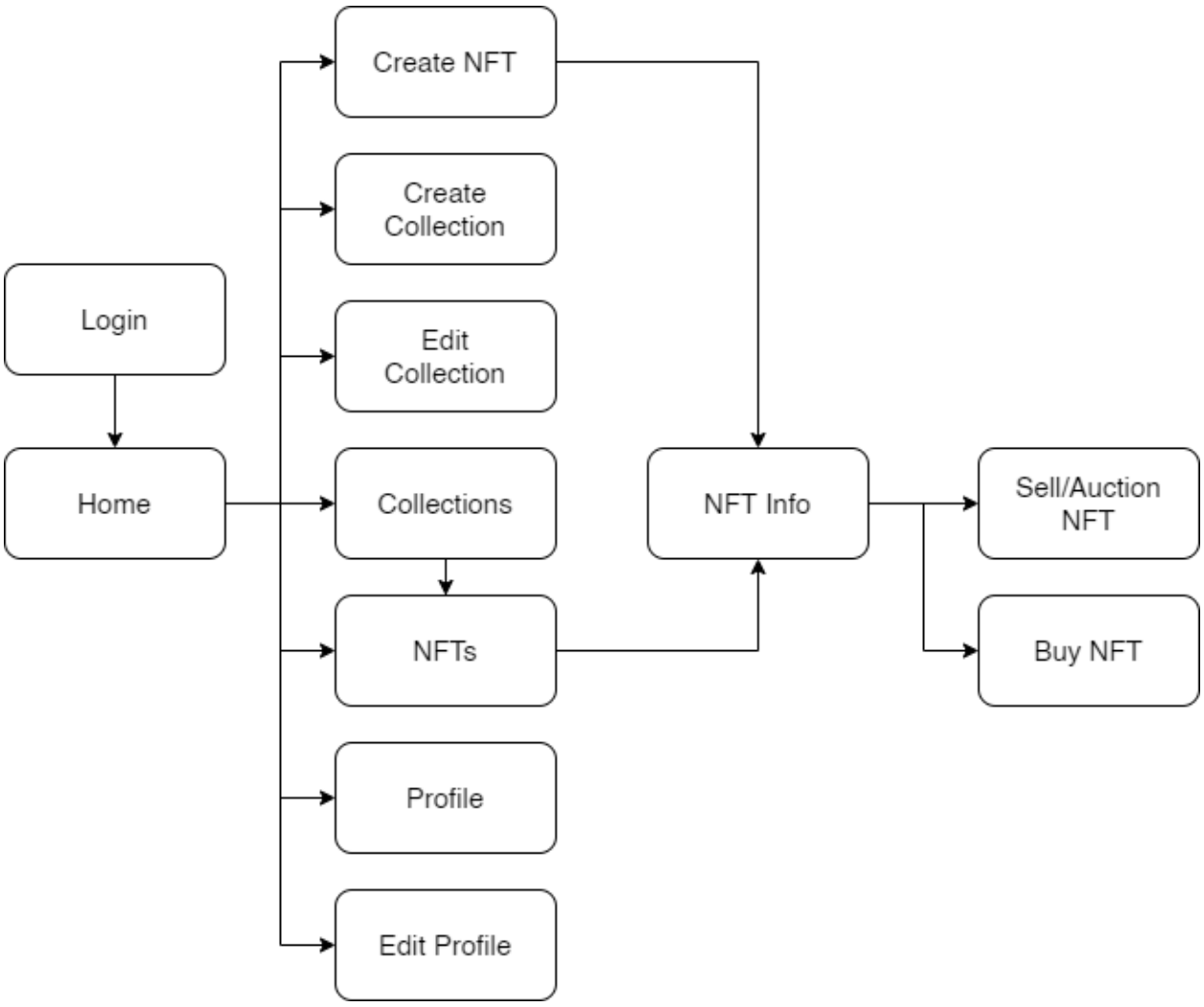
5.3. Công nghệ sử dụng

Phân hệ	Framework/Thư viện/Ngôn ngữ
Front-end	NodeJS, Next.js, Ethers.js, Web3React, Axios, Tailwindcss, NextAuth, SWR
Back-end	NodeJS, Express.js, MongoDB, Ethers.js
Database management system	MongoDB
Smart Contract	Solidity
Third-party	Metamask, Hardhat, Infura
Deployment server	Vercel, Heroku

Bảng 5-2 Bảng liệt kê công nghệ sử dụng

Chương 6 THIẾT KẾ GIAO DIỆN

6.1. Sơ đồ liên kết màn hình



Ảnh 6-1 Sơ đồ liên kết màn hình

6.2. Danh sách các màn hình

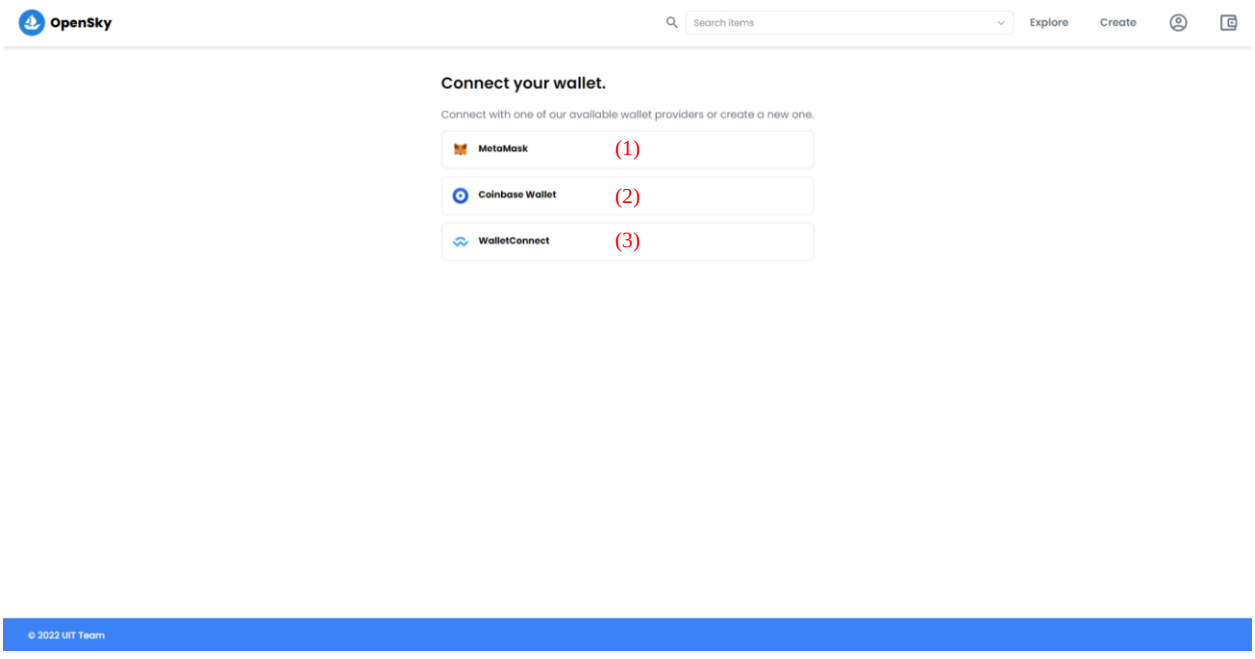
STT	Màn hình	Loại	Chức năng
1	Login	Màn hình nhập liệu	Đăng nhập tài khoản
2	Home	Màn hình hiển thị, tra cứu	Trang chủ website
3	Create NFT	Màn hình nhập liệu	Tạo mới NFT
4	Create Collection	Màn hình nhập liệu	Tạo mới bộ sưu tập NFT

5	Edit Collection	Màn hình hiển thị, chỉnh sửa	Chỉnh sửa thông tin bộ sưu tập NFT
6	Collections	Màn hình hiển thị	Xem danh sách các bộ sưu tập NFT
7	NFTs	Màn hình hiển thị	Xem danh sách các NFT
8	Profile	Màn hình hiển thị	Xem thông tin người dùng
9	Edit Profile	Màn hình hiển thị, chỉnh sửa	Chỉnh sửa thông tin người dùng
10	NFT Info	Màn hình hiển thị	Xem chi tiết thông tin NFT
11	Sell/Auction NFT	Màn hình hiển thị, nhập liệu	Đăng bán hoặc tạo đấu giá NFT
12	Buy NFT	Màn hình hiển thị, nhập liệu	Mua hoặc đấu giá NFT

Bảng 6-1 Bảng danh sách các màn hình

6.3. Mô tả chi tiết các màn hình

6.3.1. Màn hình "Login"

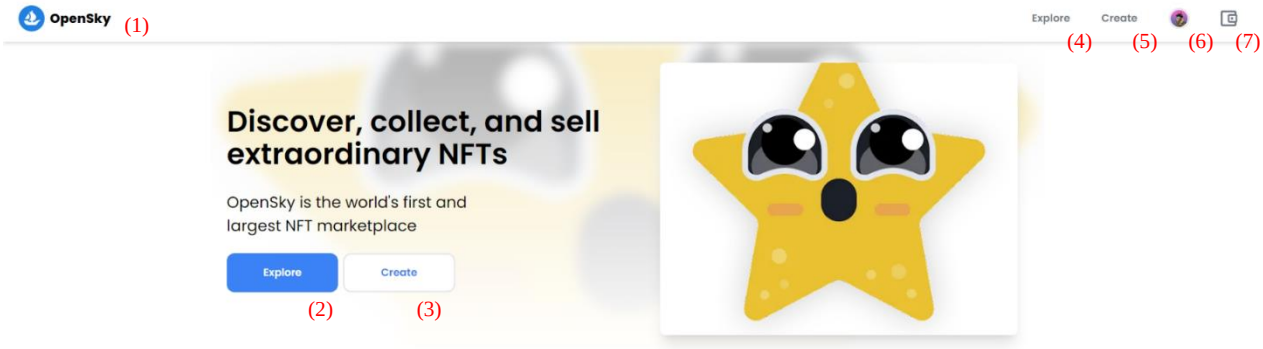


Ảnh 6-2 Màn hình "Login"

STT	Tên	Kiểu	Ý nghĩa
1	metamaskBtn	Button	Đăng nhập thông qua ví Metamask
2	coinbaseBtn	Button	Đăng nhập thông qua ví Coinbase
3	walletConnectBtn	Button	Đăng nhập thông qua ví Wallet Connect

Bảng 6-2 Bảng thành phần màn hình "Login"

6.3.2. Màn hình "Home"

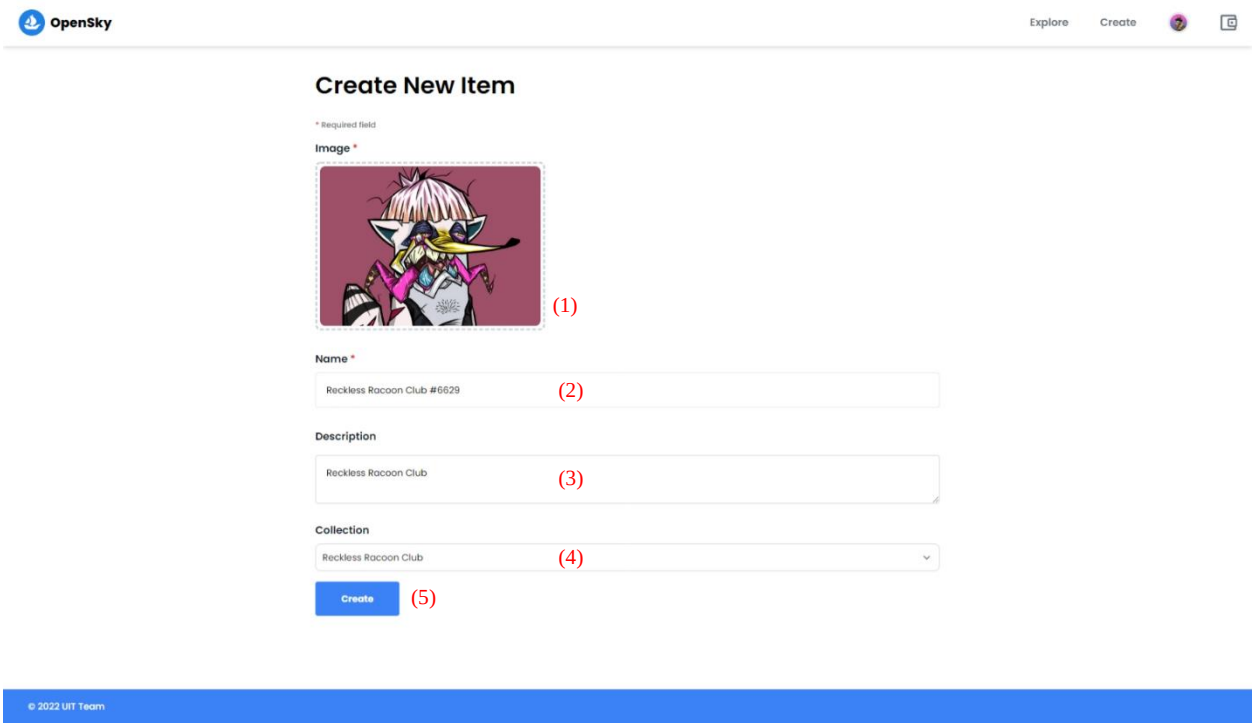


Ảnh 6-3 Màn hình "Home"

STT	Tên	Kiểu	Ý nghĩa
1	logoImg	Image	Hình ảnh logo trang web
2	exploreBtn	Button	Chuyển đến trang xem các nft và collection
3	createBtn	Button	Chuyển đến màn hình tạo nft
4	exploreNav	Button	Tương tự (2)
5	createNav	Button	Tương tự (3)
6	avatarBtn	Button	Chuyển đến màn hình thông tin user
7	walletBtn	Button	Mở drawer hiển thị thông tin ví

Bảng 6-3 Bảng thành phần màn hình "Home"

6.3.3. Màn hình "Create NFT"

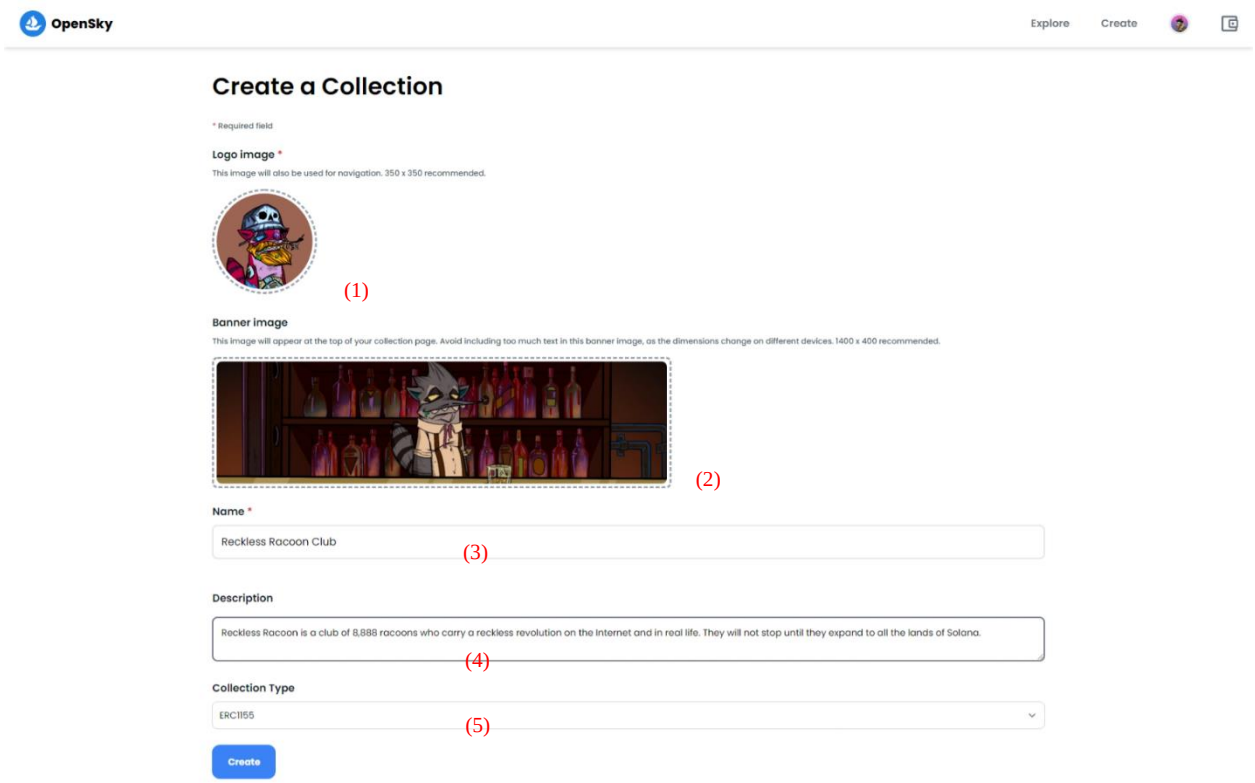


Ảnh 6-4 Màn hình "Create NFT"

STT	Tên	Kiểu	Ý nghĩa
1	nftImg	Image	Hình ảnh của NFT
2	nameText	Textfield	Tên gọi của NFT
3	descText	Textfield	Mô tả của NFT
4	collectionCb	ComboBox	Lựa chọn bộ sưu tập NFT
5	createBtn	Button	Hoàn tất tạo NFT

Bảng 6-4 Bảng thành phần màn hình "Create NFT"

6.3.4. Màn hình "Create/Edit Collection"

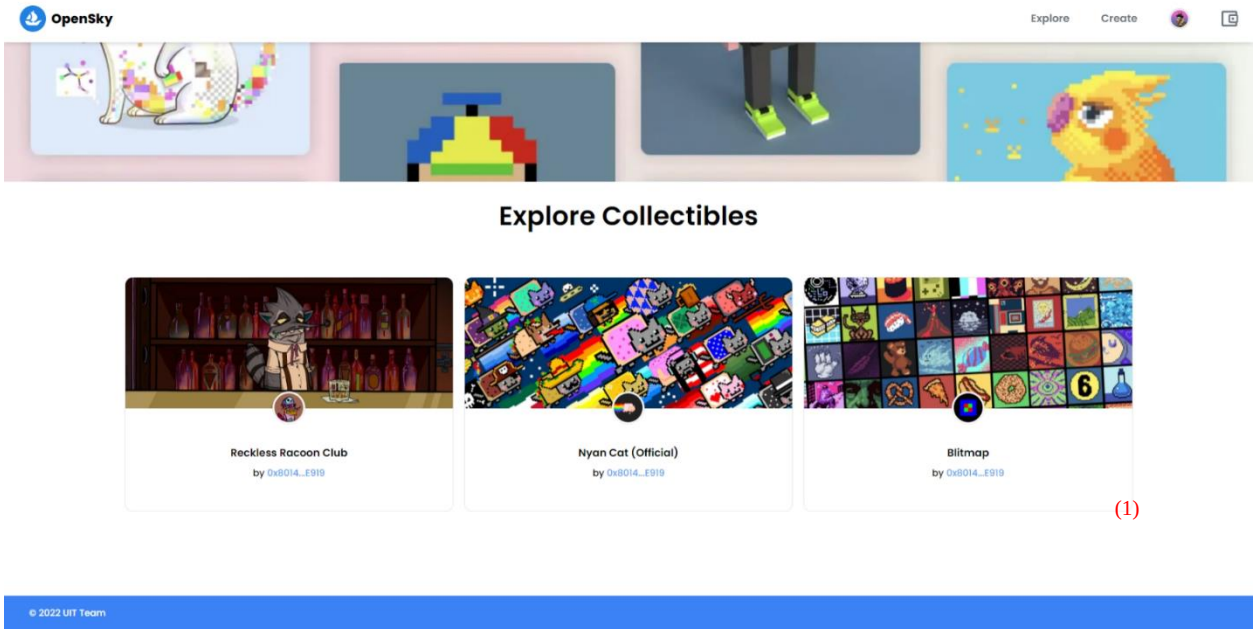


Ảnh 6-5 Màn hình "Create Collection"

STT	Tên	Kiểu	Ý nghĩa
1	cltImg	Image	Hình ảnh của bộ sưu tập
2	bannerImg	Image	Ảnh bìa của bộ sưu tập
3	nameText	Textfield	Tên của bộ sưu tập
4	descText	Textfield	Mô tả của bộ sưu tập
5	typeCb	ComboBox	Lựa chọn loại token cho bộ sưu tập
5	createBtn	Button	Hoàn tất tạo bộ sưu tập

Bảng 6-5 Bảng thành phần màn hình "Create/Edit Collection"

6.3.5. Màn hình "Collections"

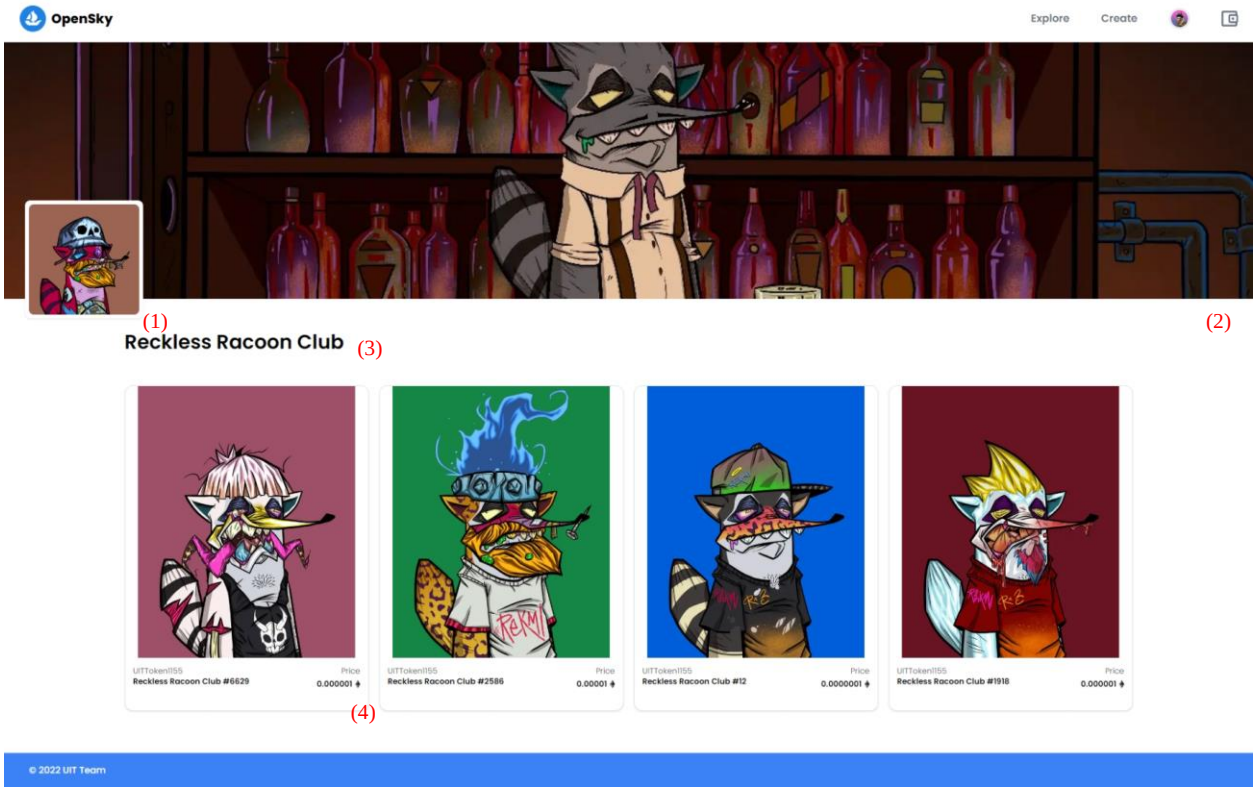


Ảnh 6-6 Màn hình "Collections"

STT	Tên	Kiểu	Ý nghĩa
1	cltCtn	Container	Hiển thị thông tin bộ sưu tập, nếu ấn vào chuyển sang trang chi tiết bộ sưu tập

Bảng 6-6 Bảng thành phần màn hình "Collections"

6.3.6. Màn hình "Collection Info"

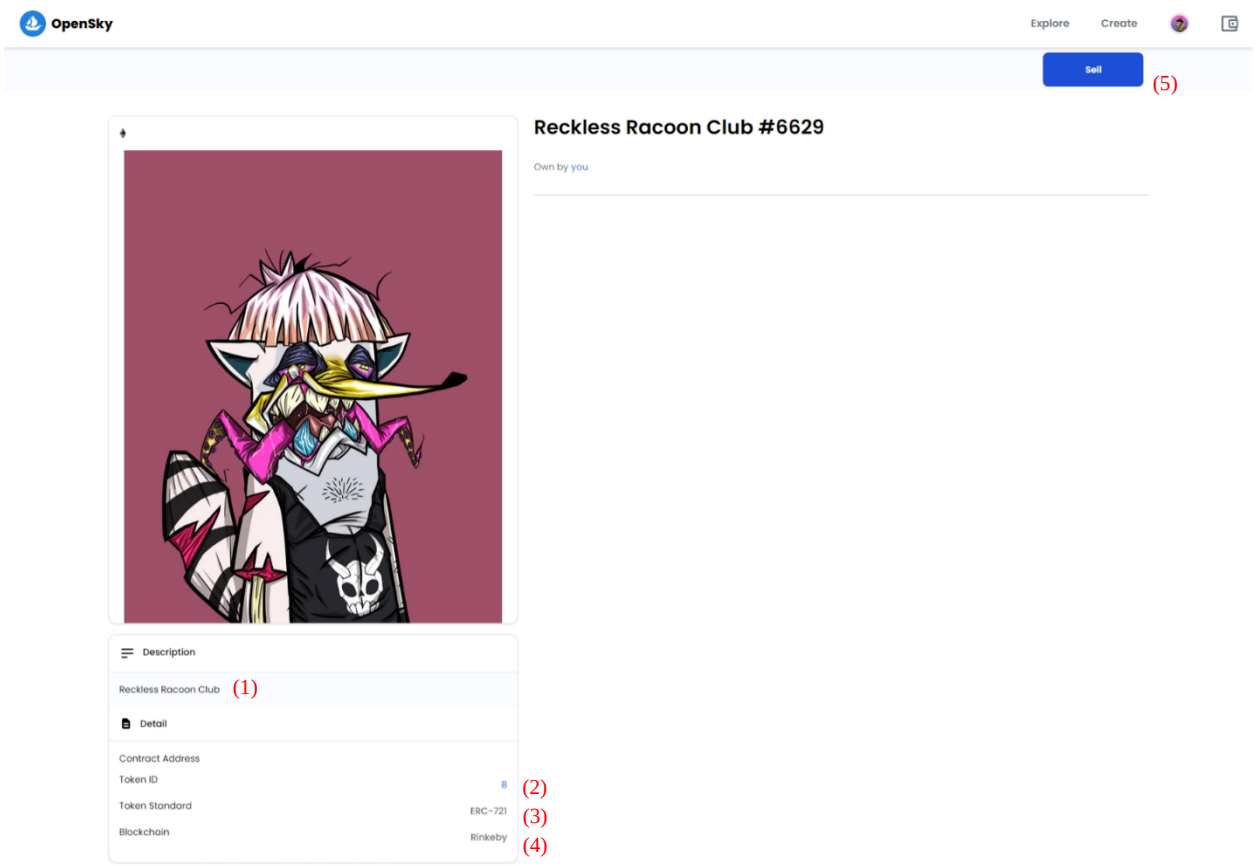


Ảnh 6-7 Màn hình "Collection Info"

STT	Tên	Kiểu	Ý nghĩa
1	cltImg	Image	Hình ảnh của bộ sưu tập
2	bannerImg	Image	Ảnh bìa của bộ sưu tập
3	nameText	Textfield	Tên của bộ sưu tập
4	nftCtn	Container	Hiển thị thông tin nft, nếu ấn vào chuyển sang trang chi tiết nft

Bảng 6-7 Bảng thành phần màn hình "Collection Info"

6.3.7. Màn hình "NFT Info"

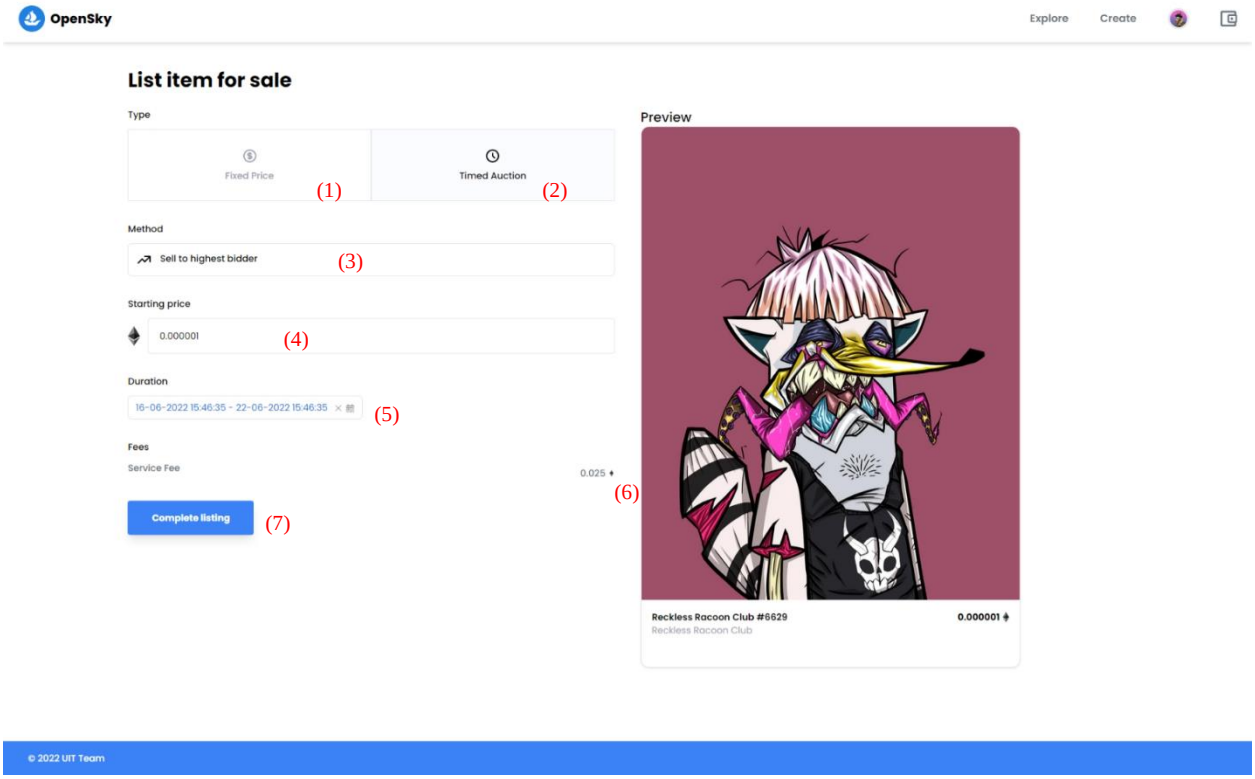


Ảnh 6-8 Màn hình "NFT Info"

STT	Tên	Kiểu	Ý nghĩa
1	descLb	Label	Hiển thị mô tả của NFT
2	idLb	Label	Hiển thị id của NFT
3	typeLb	Label	Hiển thị chuẩn token của NFT
4	networkLb	Label	Hiển thị mạng blockchain đang chứa NFT
5	sellBtn	Button	Chuyển sang trang mua, đấu giá NFT

Bảng 6-8 Bảng thành phần màn hình "NFT Info"

6.3.8. Màn hình "Sell/Create Auction NFT"

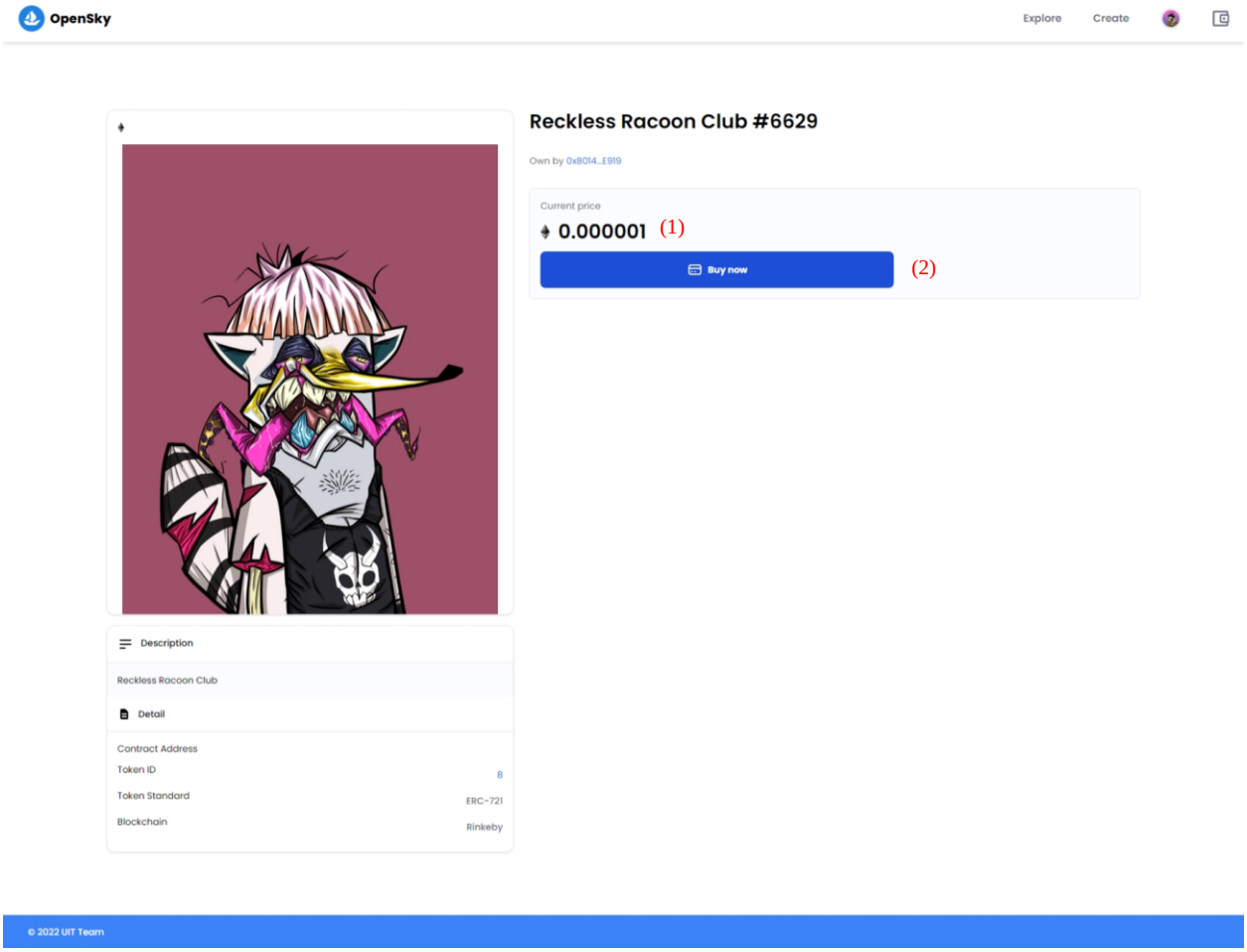


Ảnh 6-9 Màn hình "Sell/Create Auction NFT"

STT	Tên	Kiểu	Ý nghĩa
1	sellBtn	Button	Chuyển bán NFT
2	auctionBtn	Button	Chuyển sang đấu giá NFT
3	typeCb	Combobox	Chọn hình thức đấu gí
4	priceText	TextField	Nhập giá khởi điểm
5	timeDp	Datepicker	Chọn ngày bắt đầu và kết thúc
6	listingPriceLb	Label	Giá đăng đấu giá NFT
7	completeBtn	Button	Hoàn thành đấu giá NFT

Bảng 6-9 Bảng thành phần màn hình "Sell/Create Auction NFT"

6.3.9. Màn hình "Buy NFT"

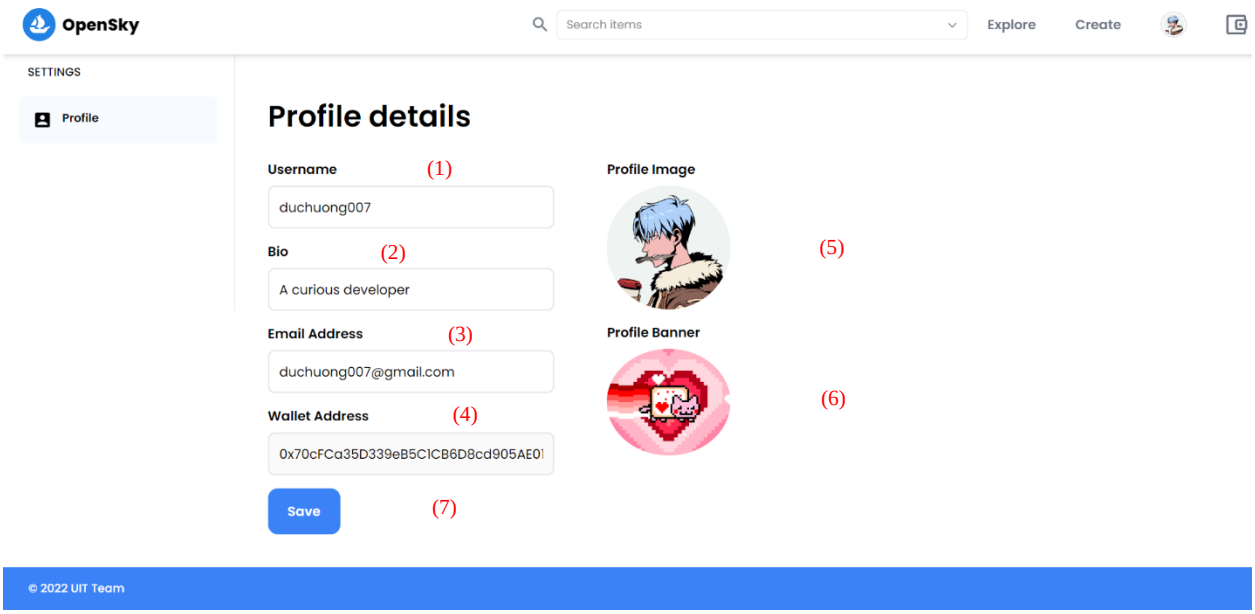


Ảnh 6-10 Màn hình "Buy NFT"

STT	Tên	Kiểu	Ý nghĩa
1	priceLb	Label	Hiển thị giá NFT
2	buyBtn	Button	Xác nhận mua NFT

Bảng 6-10 Bảng thành phần màn hình "Buy NFT"

6.3.10. Màn hình "Update User"

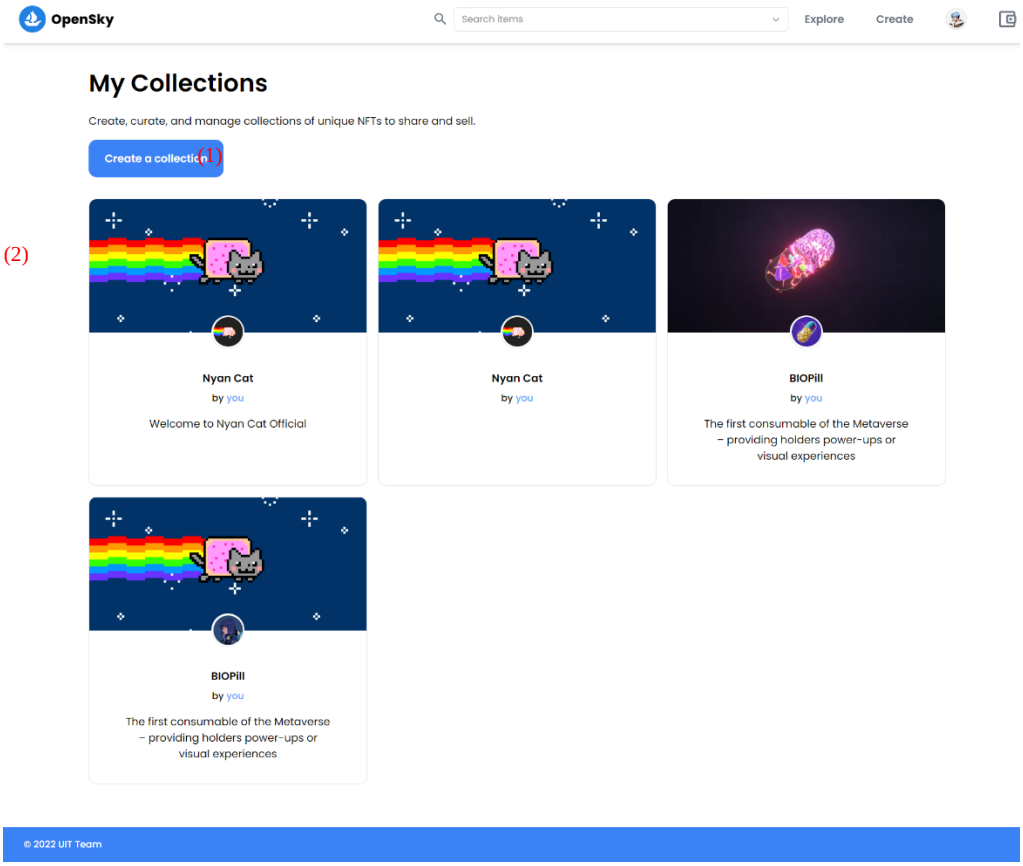


Ảnh 6-11 Màn hình "Update User"

STT	Tên	Kiểu	Ý nghĩa
1	nameText	TextField	Nhập tên của user
2	bioText	TextField	Nhập bio của user
3	emailText	TextField	Nhập địa chỉ email của User
4	walletText	TextField	Hiển thị địa chỉ của User
5	profileImage	FileInput	Thêm hình ảnh cho user
6	bannerImage	FileInput	Thêm hình banner cho trang user
7	saveButton	Button	Nút lưu thông tin cập nhật User

Bảng 6-11 Bảng thành phần màn hình "Update User"

6.3.11. Màn hình "My Collection"

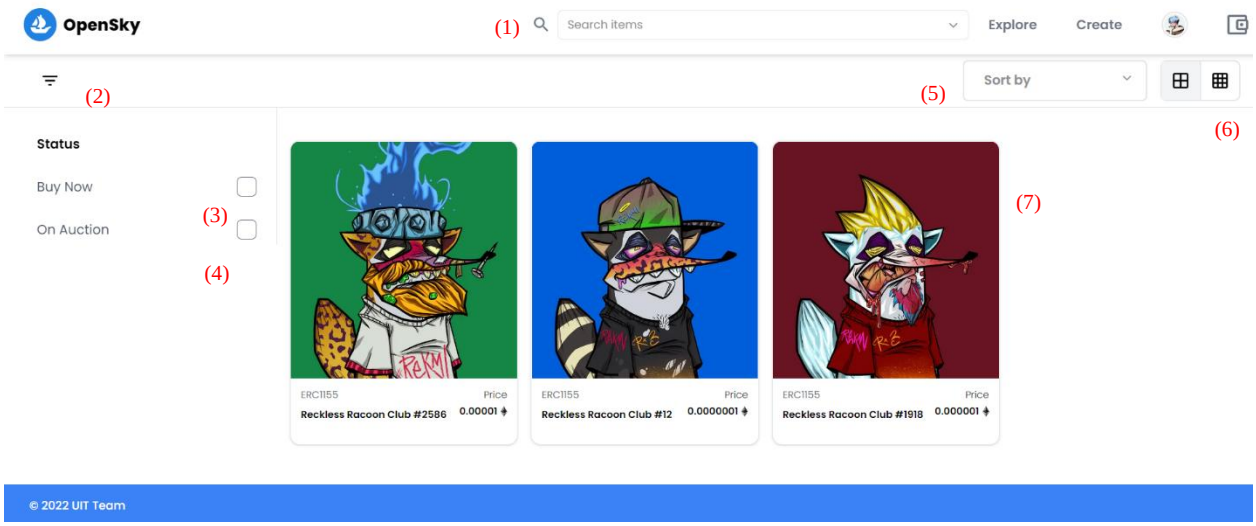


Ảnh 6-12 Màn hình "My Collection"

STT	Tên	Kiểu	Ý nghĩa
1	createBtn	Button	Tạo mới collection
2	collectionList	List	Danh sách các collection của User

Bảng 6-12 Bảng thành phần màn hình "My Collection"

6.3.12. Màn hình "All NFTs"



Ảnh 6-13 Màn hình "All NFTs"

STT	Tên	Kiểu	Ý nghĩa
1	searchText	TextField	Search các NFT
2	showBtn	Button	Ẩn / hiện thanh Filter
3	buyFilterBtn	Button	Filter các NFT đang được bán
4	auctionFilterBtn	Button	Filter các NFT đang đấu giá
5	SortCb	ComboBox	Hiển thị list thuộc tính để sort
6	GridBtn	Button	Hiển thị lưới nhỏ / to danh sách các NFT
7	NFTList	List	Danh sách các NFTs

Bảng 6-13 Bảng thành phần màn hình "All NFTs"

Chương 7 KẾT LUẬN

7.1. Kết quả đạt được

Nhóm đã nghiên cứu và áp dụng thành công công nghệ Blockchain để xây dựng thành công sàn giao dịch NFT vật phẩm ERC-721 và ERC-1155 theo cả hai phương thức mua trực tiếp lẫn đấu giá.

Nghiên cứu và xây dựng Smart Conrtact bằng Hardhat và thư viện OpenZeppelin kết hợp sử dụng Next.js, Ether.js xây dựng giao diện người dùng.

Triển khai thành công các API tương tác với cơ sở dữ liệu MongoDB được đồng bộ với dữ liệu trong smart contract giúp việc truy xuất nhanh và linh hoạt hơn. Kết hợp với thuật toán lưu trữ IPFS (thuật toán lưu trữ phân tán) giúp dữ liệu được lưu trữ vĩnh viễn một cách công khai, minh bạch.

7.2. Đánh giá

7.2.1. Thuận lợi

Giảng viên hướng dẫn tận tình hỗ trợ, đưa ra định hướng giúp nhóm thực hiện đề tài. Có sẵn nền tảng kiến thức để xây dựng ứng dụng và cơ sở hạ tầng website.

Do blockchain nói chung cũng như sàn giao dịch NFT nói riêng đang là xu hướng toàn cầu nên tài liệu về các công nghệ được chia sẻ rộng rãi.

Vận dụng được các kiến thức, quy trình phát triển đã được học giúp việc xây dựng phần mềm trở nên có hệ thống và chặt chẽ hơn.

7.2.2. Khó khăn

Khoảng thời gian đầu mới tiếp cận blockchain kiến thức còn khá mơ hồ và khó hiểu.

Tốn nhiều thời gian học ngôn ngữ mới Solidity để viết Smart Contract và cách thức deploy Smart Contract lên mạng Rinkeby.

Tìm hiểu về cách thức hoạt động của một sàn giao dịch NFT, đặc biệt là khi công nghệ blockchain và NFT còn khá mới trên thế giới nên mất nhiều thời gian để tìm hiểu và xây dựng hệ thống.

7.3. Hướng phát triển

Hoàn thiện đầy đủ các tính năng hiện tại, nâng cấp giao diện thân thiện và hiện đại hơn, giảm bớt các thao tác không cần thiết để tăng trải nghiệm người dùng.

Bổ sung thêm các hình thức đấu giá khác, liên kết thêm nhiều ví, liên kết đến các mạng xã hội, quản lý blogs người dùng…

Tái cấu trúc và nâng cao tính bảo mật của Smart Contract, hỗ trợ phát hành thêm các chuẩn token khác.

TÀI LIỆU THAM KHẢO

[1] Ethereum Development Documentation.

Available: https://ethereum.org/en/developers/docs/

[2] Ethers.js Documentation.

Available: https://docs.ethers.io/v5/

[3] Solidity Documentation.

Available: https://docs.soliditylang.org/en/v0.8.15/

[4] Hardhat – Ethereum development environment.

Available: https://hardhat.org/getting-started

[5] OpenZeppelin Documentation.

Available: https://docs.openzeppelin.com/contracts/4.x/

[6] NextAuth.js Documentation.

Available: https://next-auth.js.org/getting-started/example

[7] Mongoose.js Documentation.

Available: https://mongoosejs.com/docs/api.html