

## Sườn mục lục NCKH GAME NFT

## **LỜI CAM ĐOAN**

Chúng tôi xin cam đoan bài nghiên cứu khoa học “Cách sử dụng game card NFT để tạo trải nghiệm chơi game độc đáo và phong phú” này là công trình nghiên cứu của nhóm chúng tôi. Các nội dung được trình bày trong luận văn là hoàn toàn trung thực, không vi phạm bất cứ điều gì trong luật sở hữu trí tuệ và pháp luật Việt Nam. Những số liệu trong các bảng biểu phục vụ cho việc nhận xét, đánh giá được chính tôi thu thập từ các nguồn khác nhau và có ghi nguồn tham khảo. Nếu có bất cứ điều gì sai sót, tôi hoàn toàn chịu trách nhiệm.

**TÁC GIẢ LUẬN VĂN**

## **LỜI CẢM ƠN**

Để hoàn thành báo cáo nghiên cứu khoa học này là một quá trình đầy khó khăn và thử thách trong học tập cũng như trong quá trình nghiên cứu. Để có được những thành quả như ngày hôm nay. Tôi xin chân thành cảm ơn thầy Đinh Hoàng Gia, thầy Hồ Quý Thuận và Thầy Nguyễn Ngọc Đạt đã tận tình giúp đỡ chúng tôi cả chuyên môn, nghiên cứu và định hướng trong suốt quá trình làm luận văn. Qua đây tôi cũng xin chân thành gửi lời cảm ơn tới trường Đại học Gia Định đã tạo điều kiện cho chúng tôi được học tập và nghiên cứu, cảm ơn các thầy cô trong khoa Công nghệ thông tin đã truyền đạt những kiến thức quý báu và có giá trị, hướng dẫn chúng tôi trong suốt quá trình học tập và nghiên cứu tại trường.

Sau cùng, tôi xin chân thành cảm ơn gia đình, bạn bè đã luôn sát cánh giúp đỡ, động viên tôi trong suốt thời gian học tập và hoàn thành luận văn.

Chúng tôi xin chân thành cảm ơn!

**MỤC LỤC**  
**DANH MỤC TỪ VIẾT TẮC**  
**DANH MỤC BẢNG BIỂU**  
**DANH MỤC HÌNH ẢNH**

## LỜI MỞ ĐẦU

Công nghệ Blockchain hiện nay được coi là một công nghệ “chìa khóa” cho chuyển đổi số và xây dựng nền tảng công nghệ thông tin tương lai trong làn sóng cách mạng công nghệ 4.0. Blockchain 4.0 được thiết kế để chống lại sự thay đổi dữ liệu, lưu trữ thông tin trong các khối và các khối này liên kết với nhau theo thời gian thực tạo thành chuỗi liên tục. Sự tăng trưởng nhanh chóng trong việc áp dụng công nghệ chuỗi khối và phát triển các ứng dụng dựa trên chuỗi khối đã bắt đầu cách mạng hóa ngành tài chính và dịch vụ tài chính. Ngoài việc được công bố rộng rãi bitcoin tiền điện tử, phạm vi ứng dụng blockchain phổ biến từ các mạng độc quyền được sử dụng để xử lý các giao dịch tài chính hoặc yêu cầu bảo hiểm cho các nền tảng có thể phát hành và giao dịch vốn chủ sở hữu cổ phiếu và trái phiếu doanh nghiệp.

Ứng dụng của Blockchain trong chuyển đổi số bao gồm trong chuỗi cung ứng, công nghệ bảo hiểm insurtech, công nghệ nông nghiệp agritech, y tế, tài chính - đây được coi là huyết mạch của nền kinh tế. Bên cạnh đó nền tảng hợp đồng thông minh smart contract trong Blockchain có thể tự động hóa được nhiều quá trình, tạo ra các dịch vụ thông minh, và là một nền tảng đảm bảo an toàn cho các giao dịch số. Đặc biệt với dự báo tới năm 2025 sẽ có khoảng 75.44 tỷ thiết bị IoT tương đương với gấp 10 lần dân số thế giới, để đảm bảo tính bảo mật cho các thiết bị IoT này trao đổi, giao tiếp, chia sẻ dữ liệu với nhau thì công nghệ phù hợp, hiện đại nhất là Blockchain. Trên thế giới nói chung, công nghệ Blockchain được ứng dụng rộng rãi trong tài chính, ngân hàng, bảo hiểm, logistic, chuỗi cung ứng trong các tập đoàn lớn. Về khía cạnh chuyển đổi số, nhiều chính phủ cũng ứng dụng công nghệ Blockchain, ví dụ như tại quốc gia Georgia, cơ quan quản lý đất đai quốc gia đã chuyển việc đăng ký quyền sở hữu đất sang blockchain và hệ thống này hiện đang xử lý 160.000 hồ sơ; trong khi đó tại Estonia, chính phủ đã áp dụng công nghệ blockchain để bảo mật hồ sơ y tế và quản lý cơ sở dữ liệu của chính phủ. Mỹ, Nga đã có những đề xuất ứng dụng công nghệ Blockchain trong an ninh quốc phòng. Bởi, tính bảo mật và phi tập trung khiến blockchain phù hợp để bảo đảm an toàn cho các bản ghi dữ liệu sự kiện, hồ sơ y tế, quản lý hộ tịch, quản lý giao dịch, truy xuất nguồn gốc thực phẩm, hay trong các cuộc bầu cử bỏ phiếu. Ngoài ra, từ năm học 2020-2021, Bộ Giáo dục và Đào tạo quyết định ứng dụng công nghệ blockchain trong việc lưu trữ văn bằng quốc gia. Theo đó, tất cả văn bằng được cấp bởi

các đơn vị đào tạo thuộc Bộ Giáo dục và Đào tạo sẽ lần lượt được đưa vào hệ thống lưu trữ văn bằng quốc gia. Ngành ngân hàng, blockchain tại Việt Nam cũng được rất nhiều ngân hàng quan tâm và triển khai ứng dụng với mục tiêu cải tiến và nâng cao tính linh hoạt trong việc phát hành thư tín dụng (L/C), hợp lý hóa quy trình và cung cấp dịch vụ cho các doanh nghiệp hiệu quả nhất. Ngành y tế, từ năm 2018, Trung tâm công nghệ lõi của Viettel đã nghiên cứu ứng dụng thành công công nghệ Blockchain cho Quản lý hồ sơ bệnh án điện tử. Có thể nói, công nghệ blockchain đang phát triển rất nhanh và mạnh mẽ trong và ngoài nước, trải dài trên các lĩnh vực. Tuy nhiên, hiện tại trong Quân đội chưa có đơn vị nào công bố sản phẩm công nghệ ứng dụng Blockchain với mục đích bảo vệ dữ liệu và an ninh quốc phòng. Luận văn “*Cách sử dụng game card NFT để tạo trải nghiệm chơi game độc đáo và phong phú*” tập trung nghiên cứu về công nghệ mạng lưới của NFT, cụ thể là Polygon và Binance Smart Chain (BSC) trong quá trình bán đấu giá các sản phẩm của NFT.

Các phương pháp và công cụ nghiên cứu bao gồm:

- Nghiên cứu từ lý thuyết, các bài báo, bài nghiên cứu, hội thảo, internet về ứng dụng của công nghệ Blockchain, NFT và BSC
- Nghiên cứu thực nghiệm:
  - + Công cụ Visual Studio Code, Unity. Ngôn ngữ lập trình Typescript, Solidity, C Sharp.
  - + Nghiên cứu cài đặt,

Các nhiệm vụ chính cần thực hiện:

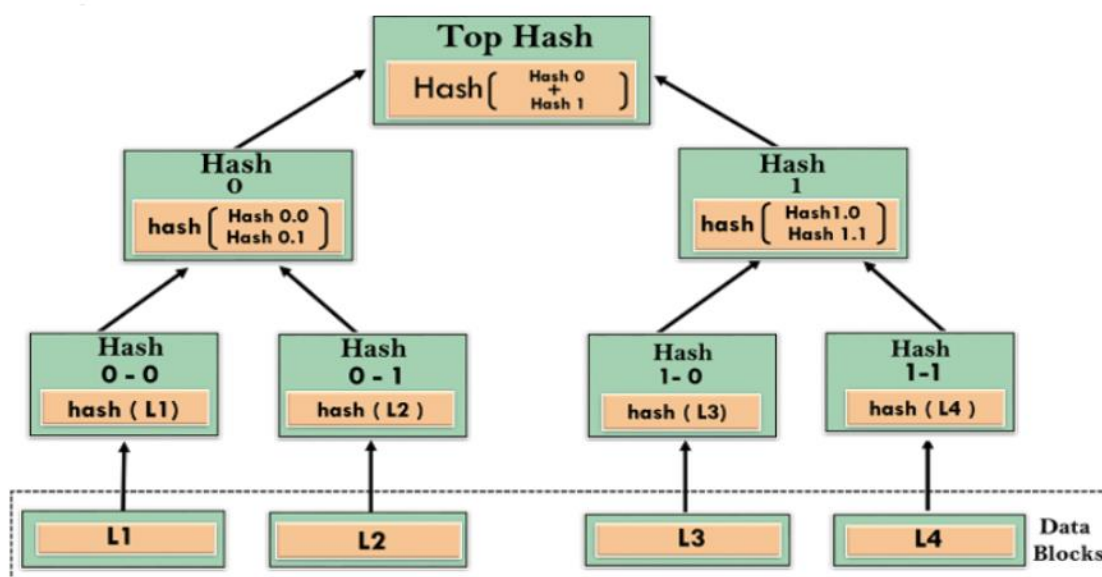
- Nghiên cứu tổng quan về công nghệ Block chain
- Nghiên cứu về Smart Contract, NFT và ứng dụng NFT
- Lựa chọn công nghệ Binance Smart Chain để làm nền tảng để xây dựng ứng dụng

# CHƯƠNG 1: TỔNG QUAN VỀ BLOCKCHAIN, NFT VÀ KHẢ NĂNG ỨNG DỤNG NFT TRONG THƯƠNG MẠI

Chương 1 trình bày tổng quan về công nghệ Blockchain, NFT và Smart Contract. Bên cạnh đó chương 1 còn trình bày về 1 số vấn đề bảo mật của NFT và ứng dụng NFT trong thương mại điện tử ngày nay.

## 1.1. Tổng quan về công nghệ Blockchain 1.1.1. Lịch sử hình thành

Vào năm 1976, một bài báo được phát hành có tên là “*New Directions in Cryptography*” đã thảo luận về khái niệm sổ cái phân tán và cùng với sự tiến bộ trong lĩnh vực Mật mã học, một bài báo có tiêu đề là “*Hot to Time-Stamp a Digital Document*” của Stuart Haber và Scott Stornetta đã đặt ra khái niệm để đánh dấu thời gian dữ liệu thay vì phương tiện. Một khái niệm quan trọng khác được gọi là “*Electronic cash*” hay “*Digital Currency*” ra đời dựa trên một mô hình do David Chaum đề xuất cũng đóng góp cho sự phát triển của khái niệm Blockchain, theo sau là các giao thức như các chương trình tiền điện tử. Năm 1992, Merkle Trees được tích hợp vào thiết kế, tạo nên chuỗi khối hiệu quả hơn bằng cách cho phép thu thập một số tài liệu vào một khối. Thuật toán Merkle Trees được sử dụng để tạo ra một blockchain an toàn, sử dụng để lưu trữ một loạt các bản ghi dữ liệu và mỗi bản ghi dữ liệu được kết nối với một bản ghi trước nó. Bản ghi mới nhất trong chuỗi chứa lịch sử của toàn bộ chuỗi. Tuy nhiên, công nghệ này không được sử dụng và bằng sáng chế đã hết hiệu lực vào năm 2004.



Hình 1 1: Mô tả về chuỗi khối mật mã tích hợp Merkle Trees

Satoshi Nakamoto được coi là người phát minh ra công nghệ block chain khi ông xuất bản một bài báo về bitcoin vào năm 2008 với tên gọi "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Bản tóm tắt của bài báo được phát trực tiếp trên mạng thanh toán từ nguồn này sang nguồn khác mà không dựa vào trên một nguồn của bên thứ ba. Bài báo mô tả một thiết bị điện tử hệ thống thanh toán dựa trên khái niệm Mật mã. Bài báo của Nakamoto đã cung cấp một giải pháp cho vấn đề chi tiêu kép khi một loại tiền kỹ thuật số không thể bị sao chép và không ai có thể chi tiêu nó nhiều hơn một lần. Một chương trình nguồn mở để triển khai hệ thống bitcoin được phát hành chỉ sau vài tháng sau đó và mạng bitcoin đầu tiên được bắt đầu vào đầu năm 2009 khi Satoshi Nakamoto đã tạo ra những bitcoin ban đầu. Có hàng trăm loại tiền điện tử khác nhau như Litecoin, Dogecoin,... nhưng bitcoin nắm giữ phần lớn thị trường nó đã trở thành loại tiền điện tử phổ biến nhất. Nó đã thu hút sự chú ý của người dùng do khả năng giữ sự nhất trí cho người dùng, nhưng nó đã trở nên thực sự phổ biến do tính minh bạch của nó. Bitcoin bắt đầu khởi sắc kể từ đó và đến năm 2013, các nhà đầu tư bắt đầu đổ tiền vào các công ty khởi nghiệp liên quan đến Bitcoin. Bitcoin có thể được đổi lấy tiền tệ thông thường, cho bất kỳ dịch vụ hoặc sản phẩm nào. Với việc sử dụng phần mềm ví điện tử, người dùng có thể chuyển bitcoin bằng máy tính, điện thoại di động hoặc ứng dụng Web. Vào năm 2015, nền tảng Ethereum đã được ra mắt cho phép blockchain hoạt động với các khoản vay và danh bạ, đó là dựa trên một thuật toán được gọi là Hợp đồng thông minh đảm bảo thực hiện một hành động giữa hai bên. Bởi vì Ethereum có khả năng cung cấp dịch vụ nhanh hơn, an toàn hơn và môi trường hiệu quả hơn, công nghệ này đã trở nên phổ biến rộng rãi.

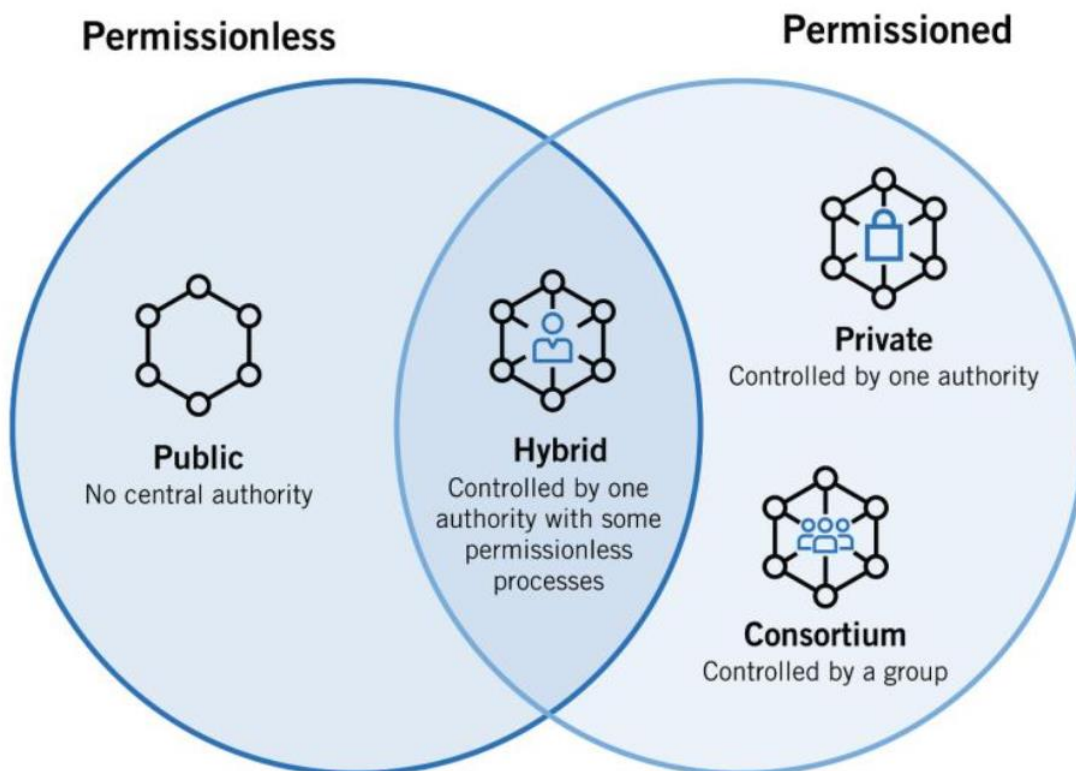
### **1.1.2. Khái niệm**

Blockchain là một cơ sở dữ liệu phân tán được chia sẻ giữa các nút của mạng máy tính, một blockchain lưu trữ thông tin điện tử ở định dạng kỹ thuật số. Blockchains được biết đến nhiều nhất với vai trò quan trọng trong các hệ thống tiền điện tử, chẳng hạn như Bitcoin, để duy trì hồ sơ giao dịch an toàn và phi tập trung. Sự đổi mới với blockchain là nó đảm bảo tính trung thực và bảo mật của bản ghi dữ liệu và tạo ra sự tin cậy mà không cần đến bên thứ ba đáng tin cậy. Một Blockchain thu thập thông tin với nhau thành các nhóm, được gọi là các khối, chứa tập hợp thông tin. Các block có khả năng lưu trữ nhất định và khi được lấp đầy, block sẽ đóng lại và liên kết với block đã được lấp đầy trước đó, tạo thành một chuỗi dữ liệu được gọi là Blockchain. Tất cả thông tin mới theo sau block mới thêm được biên dịch thành một block mới được hình thành, sau đó cũng sẽ được thêm vào chuỗi sau khi được lấp đầy.

Cấu trúc dữ liệu của Blockchain thành các phần (block) được xâu chuỗi lại với nhau. Cấu trúc dữ liệu này tạo ra dòng thời gian không thể thay đổi của dữ liệu khi được thực hiện theo bản chất phi tập trung. Khi một khối được lấp đầy, nó sẽ được đặt cố định và trở thành một phần của dòng thời gian. Mỗi khối trong chuỗi được cấp một dấu thời gian chính xác khi được thêm vào chuỗi.

Blockchain được phân ra thành 3 loại chính:





Hình 1.2: 3 loại block chain

### *Public Blockchain*

Mạng Blockchain mở đối với tất cả người dùng, người dùng có thể truy cập hoặc truy vấn vào mạng public blockchain. Người dùng có thể có quyền tải mã lập trình và chạy nút công khai trên thiết bị. Ngoài ra, người ngoài có thể kiểm tra trạng thái hiện tại và có thể quyết định thêm khối khác vào chuỗi. Hệ thống hay máy chủ không yêu cầu phí bảo trì, do đó các ứng dụng phi tập trung không tốn nhiều chi phí để tạo và vận hành. Một trong những mạng public blockchain hàng đầu là Bitcoin, Ethereum, Dash, Dogecoin, Litecoin, Monero.

### *Federated Blockchains (Consortium Blockchains)*

Mạng Federated Blockchain có cơ chế phân quyền, người dùng không có quyền truy cập vào sổ cái, quyền đọc và các quy trình xác minh giao dịch. Mạng Blockchain này hình thành do một nhóm các nhà lãnh đạo tạo ra, do đó tính bảo mật, riêng tư của giao dịch và khả năng mở rộng được đánh giá cao hơn public Blockchain. Nhóm quản trị của mạng Blockchain kiểm soát tất cả các quá trình đồng thuận, thường được sử dụng trong ngân hàng. Người dùng bình thường sẽ không có quyền tham gia vào hệ thống nếu như không được xác thực ủy quyền từ người quản trị. Một số ví dụ về Federated Blockchains là B3i (Bảo hiểm), R3 (Ngân hàng), Corda, EWWF (Năng lượng).

### *Private Blockchains*

Private Blockchain là mạng lưới Blockchain trong đó một tổ chức duy nhất nắm toàn quyền về những người có thể tham gia mạng, truy cập vào nút và tham gia

vào thuật toán đồng thuận hay nói cách khác, tổ chức có toàn quyền kiểm soát mạng. Do tính chất này, Private Blockchain còn được gọi là một Permissioned Blockchain (Blockchain được phân quyền). Cơ chế hoạt động trên một sổ cái phân tán và người dùng có quyền có toàn quyền truy cập vào các nút. Private Blockchain đem lại hiệu quả cao hơn, khả năng mở rộng tốt hơn và bảo mật mạnh mẽ.

### **1.1.3. Tính năng**

#### *Cấu trúc dữ liệu chặt chẽ*

Blockchain là một bản ghi dữ liệu đang phát triển, được biên dịch dưới dạng các khối ảo. Trong blockchain của Bitcoin, dữ liệu được ghi lại là các giao dịch Bitcoin. Cấu trúc bắt đầu với một khối duy nhất được gọi là khối gốc (Genesis block). Khi lượng dữ liệu được ghi trên hệ thống tăng lên, các khối tiếp tục được tạo ra và thêm vào chuỗi. Mỗi khối trong chuỗi được liên kết với khối trước, sau đó đưa dữ liệu quay trở lại khối gốc.

Cấu trúc dữ liệu về danh sách liên kết đã được nghiên cứu và sử dụng trong công nghệ thông tin nhiều thập kỷ qua. Nhiều ứng dụng xử lý văn bản và ảnh tạo các ngăn xếp dữ liệu được liên kết tuần tự, vì vậy người dùng có thể “hoàn tác” trạng thái gần đây nhất và hoàn nguyên về trạng thái trước đó. Tuy nhiên, blockchain được thiết kế để trở thành bằng chứng bất biến, không thể đảo ngược và giả mạo.

#### *Tính bất biến và chống giả mạo trong Blockchain*

Dữ liệu được lưu trữ trong chuỗi khối được đảm bảo an toàn và bất biến bằng cách sử dụng mật mã. Mỗi khối được tham chiếu bởi một chuỗi ký tự duy nhất, được tạo bởi một hàm băm mật mã. Hàm này chấp nhận bất kỳ lượng dữ liệu nào làm đầu vào và tạo ra một chuỗi có độ dài cố định làm đầu ra. Đầu ra có độ dài cố định này được gọi là một hàm băm. Mỗi khối liên kết với khối trước (được gọi là khối cha) bằng cách lưu trữ hàm băm của khối cha. Một trong những đặc tính nổi bật của hàm băm là một thay đổi nhỏ trong đầu vào cũng tạo ra đầu ra băm hoàn toàn khác. Do đó, bất kỳ thay đổi nào được thực hiện đối với nội dung sẽ thay đổi hàm băm của khối, mỗi khối lưu trữ hàm băm của khối cha. Do đó, việc giả mạo dữ liệu trong bất kỳ khối nào trên Blockchain sẽ thay đổi hàm băm của tất cả các khối tiếp theo. Bằng cách này, người dùng có thể xác định giả mạo tại bất kỳ điểm nào trên chuỗi khối mà không cần phải xác minh nội dung của từng khối. Điều này tạo ra những ứng dụng mạnh mẽ ngoài tiền điện tử. Việc phát hiện giả mạo đem lại hữu ích trong việc kiểm tra cơ sở dữ liệu trực tuyến về các tài sản vật chất có giá trị, chẳng hạn như bất động sản hay nghệ thuật.

#### *Dữ liệu được bảo mật trong Blockchain*

Mỗi đồng Bitcoin được lưu trữ trên chính blockchain thay vì một tài khoản vật lý hoặc tài khoản trực tuyến được duy trì bởi bên thứ ba (chẳng hạn như ngân hàng). Người dùng có thể truy cập Bitcoin an toàn bằng các cặp khóa riêng tư/công khai. Người tiêu dùng có thể giao dịch hoặc chuyển đổi bitcoin của mình bằng khóa riêng, trong khi người bán nhận bitcoin bằng cách chia sẻ khóa công khai với người mua. Khi giao dịch đã được chuyển tiếp trên mạng internet và nằm

trong một khối sẽ được coi là vĩnh viễn. Sau đó, người bán có thể yêu cầu quyền sở hữu không thể chối cãi hoặc sử dụng khóa riêng để sử dụng Bitcoin.

Blockchain thường được lưu trữ và duy trì trên nhiều thiết bị, hàng nghìn thiết bị trên toàn thế giới lưu trữ chuỗi khối của Bitcoin. Do đó, dữ liệu được bảo vệ ngay cả khi một hoặc nhiều thiết bị bị xâm nhập bởi các cuộc tấn công hoặc các sự cố mạng.

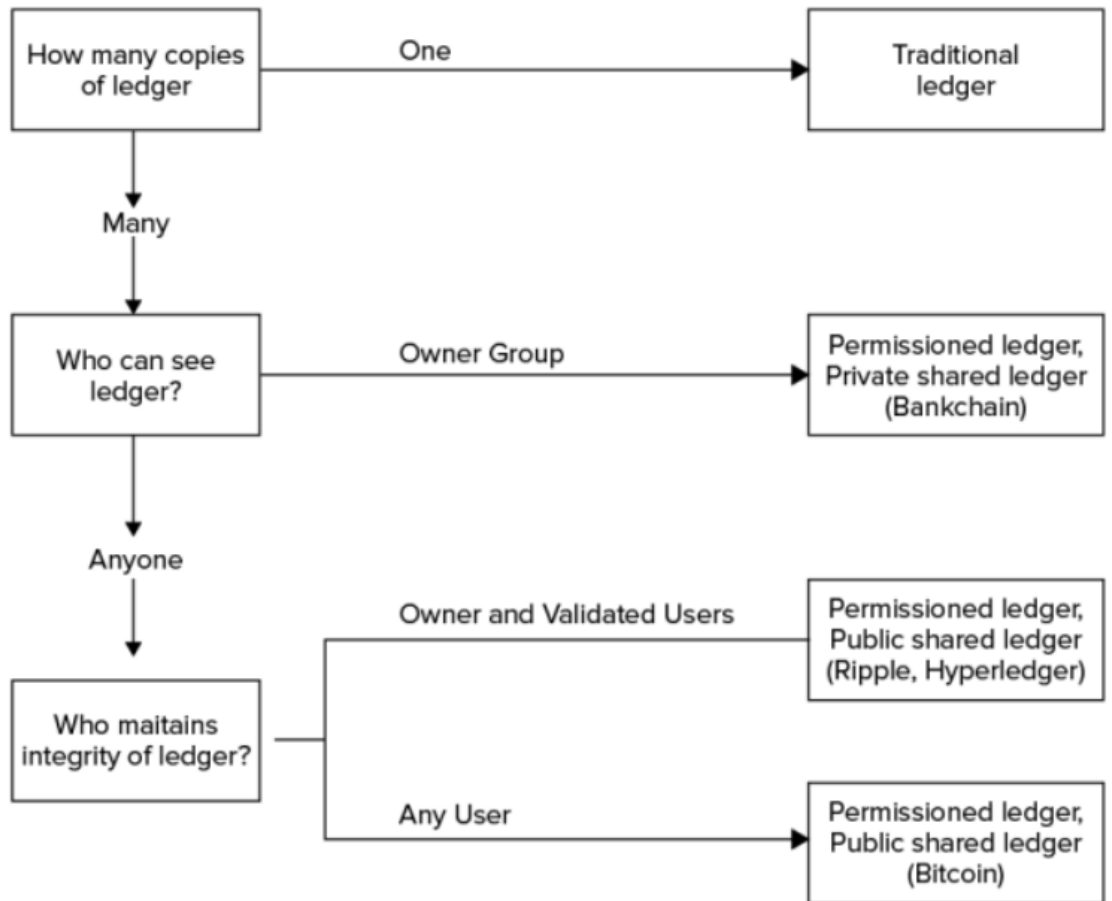
### *Công nghệ sổ cái phân tán*

Sổ cái được chia sẻ giữa một nhóm người dùng riêng tư được kết nối qua mạng cục bộ hoặc với người dùng trên internet. Thông báo được tạo ra và chuyển tiếp khi hình thành nên mỗi khối mới để đảm bảo rằng tất cả người dùng đều có phiên bản mới nhất của sổ cái. Tính năng này có các ứng dụng vượt xa các loại tiền điện tử dựa vào cơ chế loại bỏ trung tâm tin cậy để ghi lại thông tin. Các ứng dụng về hệ thống phân tán bao gồm sàn giao dịch chứng khoán, giao dịch bất động sản, nhận dạng thông tin cá nhân và nhiều lĩnh vực khác.



*Hình 1.3: Mô tả về công nghệ sổ cái phân tán*

Hệ thống mạng phân tán giúp cho Blockchain không cần các cơ quan quản lý hoặc người quản lý nào riêng biệt, hay bao gồm các nút duy trì mạng. Do sổ cái được lưu trữ trên nhiều thiết bị lưu trữ ở các vị trí khác nhau, nên cũng bảo vệ hệ thống khỏi bị mất dữ liệu trong trường hợp bất kỳ thiết bị hoặc máy chủ nào gặp sự cố. Công nghệ Blockchain tách rời việc quản trị tập trung và phân chia đều cho các nút mạng để xử lý tính toán. Mỗi nút mạng sẽ lưu trữ một bản sao hoàn chỉnh của toàn bộ Blockchain. Khi muốn thay đổi nội dung của một khối, blockchain sẽ thay đổi toàn bộ hàm băm của các khối bên trong.



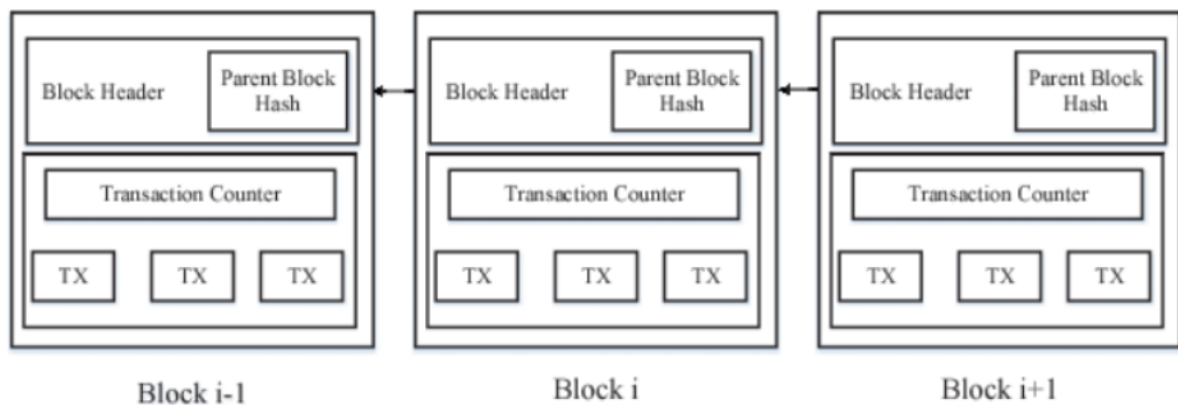
Hình 1.4: Phân loại sổ cái phân tán theo từng

### *Ẩn danh người dùng*

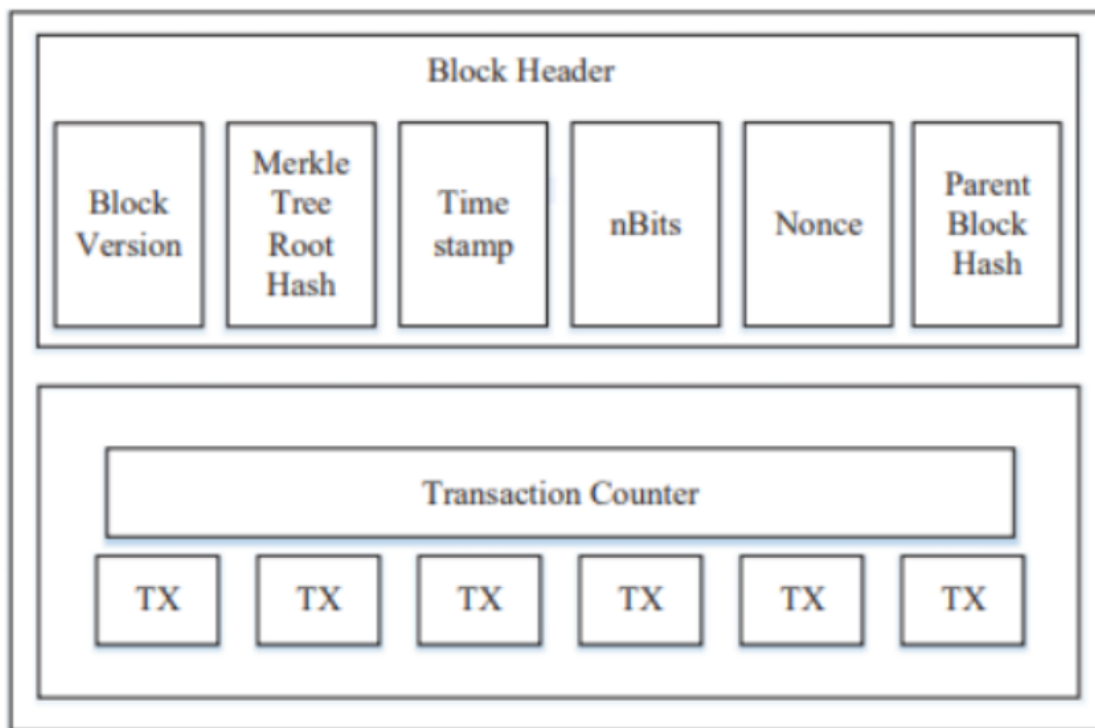
Blockchain chỉ hiển thị các địa chỉ số với các đơn vị tương ứng để ẩn danh người dùng. Việc sử dụng mật mã khóa công khai cho phép chia sẻ Blockchain trên toàn cầu trong khi vẫn duy trì tính ẩn danh tương đối do các giao dịch được ghi lại vĩnh viễn trên Blockchain. Vì chuỗi khối Bitcoin công khai, lịch sử giao dịch của người dùng sẽ bị theo dõi nếu lộ địa chỉ Bitcoin

#### **1.1.4. Kiến trúc**

Blockchain là một chuỗi các khối, chứa danh sách đầy đủ các hồ sơ giao dịch giống như sổ cái công khai thông thường. Với mã băm khối trước được chứa trong header của khối, một khối chỉ có một khối cha. Điều đáng chú ý là hàm băm của các khối chú (con của tổ tiên khối) cũng sẽ được lưu trữ trong chuỗi khối ethereum. Khối đầu tiên của một blockchain được gọi là khối genesis không có khối cha.



*Hình 1.5: Mô hình các khối liên tục trong Blockchain*



Hình 1.6: Cấu trúc khối Blockchain

### Khối (Block)

Cấu trúc khối bao gồm tiêu đề khối (Block header) và nội dung khối (Block body). Cụ thể, tiêu đề khối bao gồm:

- + Phiên bản của khối (Block version): Xác định bộ quy tắc xác thực khối cần tuân theo
- + Mã băm gốc cây Merkle (Merkle tree root hash): Chứa giá trị băm của tất cả các giao dịch trong khối
- + Dấu thời gian (Timestamp): Thời gian hiện tại tính bằng giây theo thời gian quốc tế tính từ mốc ngày 1 tháng 1 năm 1970+ nBits: Ngưỡng mục tiêu của hàm băm khối hợp lệ
- + Nonce: trường 4 byte, thường bắt đầu bằng 0 và tăng lên cho mọi phép toán băm.
- + Mã băm của khối cha (Parent block hash): giá trị băm 256 bit trỏ đến khối trước.

Phần nội dung khối (block body) bao gồm thành phần quản lý giao dịch (Transaction Counter) và các giao dịch. Số lượng giao dịch tối đa mà một khối có thể chứa tùy thuộc vào kích thước khối và quy mô của mỗi giao dịch. Blockchain sử dụng cơ chế mật mã không đối xứng để xác nhận tính xác thực của các giao dịch. Chữ ký điện tử dựa trên mật mã không đối xứng được sử dụng trong một môi trường không tin cậy.

### *Chữ ký điện tử (Digital Signature)*

Mỗi người dùng sở hữu một cặp khóa riêng tư và khóa công khai. Khóa riêng tư được giữ bí mật để sử dụng để ký kết các giao dịch. Các giao dịch đã ký số được phát trên toàn bộ mạng. Chữ ký điện tử bao gồm hai giai đoạn: giai đoạn ký và giai đoạn xác minh. Ví dụ: Người dùng Alice muốn gửi cho Bob một tin nhắn. (1) Trong giai đoạn ký, Alice mã hóa dữ liệu bằng khóa riêng của cô ấy và gửi cho Bob kết quả được mã hóa và dữ liệu gốc. (2) Trong giai đoạn xác minh, Bob xác thực giá trị bằng khóa công khai của Alice. Bằng cách đó, Bob có thể dễ dàng kiểm tra tính giả mạo của dữ liệu. Thuật toán chữ ký số được sử dụng trong blockchain là thuật toán chữ ký số theo đường cong elliptic (ECDSA).

#### **1.1.5. Thuật toán đồng thuận (Consensus Algorithms)**

Trong blockchain, để đạt được sự đồng thuận giữa các nút là một sự chuyển đổi của Bài toán Byzantine Generals (BG) - đạt được sự đồng thuận trong môi trường Blockchain phân tán. Tại blockchain, không có nút trung tâm chịu trách nhiệm đảm bảo số cái trên các nút phân tán đều giống nhau. Một số giao thức cần thiết để đảm bảo số cái ở các nút khác nhau là nhất quán. Một số cách tiếp cận phổ biến để đạt được sự đồng thuận trong blockchain bao gồm:

*PoW (Proof of work)*: là một cơ chế đồng thuận được sử dụng trong mạng Bitcoin. Trong mạng lưới phi tập trung, một người phải được chọn để ghi lại các giao dịch. Cách dễ nhất là lựa chọn ngẫu nhiên nhưng rất dễ bị tấn công. Vì vậy, nếu một nút muốn tạo ra một khối giao dịch, nút phải được thực hiện để chứng minh rằng không có khả năng bị tấn công mạng, hay còn gọi là tính toán máy tính. Trong PoW, mỗi nút của mạng tính toán giá trị băm của tiêu đề khối (Block Header). Tiêu đề khối chứa một nonce và người khai thác sẽ thay đổi nonce thường xuyên để nhận được các giá trị băm khác nhau. Sự đồng thuận yêu cầu giá trị được tính toán phải bằng hoặc nhỏ hơn một giá trị nhất định cho trước. Khi một nút đạt đến giá trị đích, tạo ra thông báo khối tới các nút khác và tất cả các nút khác phải cùng nhau xác nhận tính đúng đắn của giá trị băm. Nếu khối được xác thực, những người khai thác khác sẽ nối khối mới này vào chuỗi khối của riêng họ. Các nút tính toán giá trị băm được gọi là công cụ khai thác và quy trình PoW được gọi là khai thác bằng Bitcoin.

*PoS (Proof of Stake)*: là một giải pháp thay thế tiết kiệm năng lượng cho PoW. Người khai thác trong PoS phải chứng minh quyền sở hữu số lượng tiền tệ. Cơ chế lựa chọn dựa trên số dư tài khoản được coi là không công bằng vì người giàu nhất thường chiếm ưu thế trong mạng lưới. Do đó, nhiều giải pháp được đề xuất với sự kết hợp của kích thước stake để quyết định thành phần sẽ tạo ra khối tiếp theo. So với PoW, PoS tiết kiệm năng lượng hơn và hiệu quả hơn. Tuy nhiên, do chi phí khai thác gần như bằng 0, nên các cuộc tấn công vẫn có thể xảy ra. Nhiều blockchain áp dụng PoW ngay từ đầu và dần dần chuyển đổi sang PoS. Ví dụ, ethereum đang có kế hoạch chuyển từ Ethash (PoW) sang Casper (PoS).

*CFT (crash fault-tolerance)*: các thuật toán chịu lỗi thông thường, khi xảy ra sự cố hệ thống trong mạng Blockchain, ổ đĩa hoặc máy chủ, vẫn có thể đạt được thỏa

thuận về một đề xuất. Các thuật toán CFT cổ điển bao gồm Paxos và Raft có hiệu suất tốt hơn và chịu được ít hơn một nửa số nút gặp sự cố.

**BFT (Byzantine fault-tolerant):** Thuật toán chịu được lỗi Byzantine như gian lận nút (giả mạo kết quả thực hiện của giao dịch) bên cạnh các sự cố xảy ra trong quá trình đồng thuận. Thuật toán BFT cổ điển bao gồm PBFT, có hiệu suất thấp và chịu được ít hơn một phần ba số nút trực trực.

## **1.2. Tổng quan NFT và Smart Contract**

### **1.2.1. Lịch sử ra đời NFT**

Những ý tưởng đầu tiên tương tự như NFT đã có từ năm 2012. Lúc đó, Yoni Assia lần đầu công bố *Colored Coin* trên Blockchain Bitcoin với giá chỉ một *Satoshi* – đơn vị nhỏ nhất của Bitcoin. Tuy còn khá đơn giản nhưng vào thời điểm hiện nay, ý tưởng về *Colored Coin* đã có khá nhiều điểm tương đồng với NFT bây giờ, đó là sử dụng Blockchain làm giấy chứng nhận quyền sở hữu cho các tài sản như cổ phiếu, đồ sưu tầm kỹ thuật số, vé xem đá bóng,... Nhưng đáng tiếc rằng *Colored Coin* ngay lập tức thất bại vì một lý do Bitcoin không được tạo ra để hỗ trợ loại hình này.

Năm 2014, một nền tảng chính tương tự với mã nguồn mở có tên *Counterparty* ra đời. Nó được xây dựng trên nền tảng của Blockchain Bitcoin nhưng với nhiều cải tiến hơn. Đây có thể coi là nền tảng Bitcoin 2.0 đầu tiên và cũng là địa chỉ để người dùng tạo ra tiền tệ hoặc tài sản có thể giao dịch. *Counterparty* lúc đó rất nổi tiếng với các giao dịch mua bán meme Éch Pepe.

Năm 2017, ERC – 721 xuất hiện, đây được xem là một trong những bước ngoặt lớn của nền tảng token. ERC – 721 cho phép phát hành và giao dịch các tài sản trên Blockchain Ethereum. Điều đó có nghĩa là các nền tảng của bên thứ 3 như *Counterparty* không còn cần thiết khi giao dịch các loại tài sản nữa. Lúc này, người ta cũng bắt đầu gọi tên cho hình thức này là NFT. Ethereum hoàn thiện NFT và trở thành người dẫn đầu thị trường tài sản được lưu trữ trên Blockchain. NFT dần được nhiều người biết đến qua game nuôi mèo ảo *Crypto Kitties*, cho phép người chơi nuôi, giao dịch mèo ảo bằng đồng Ether.

### **1.2.2. Khái niệm NFT**

NFT viết tắt của “*Non-Fungible ToKens*”, là tài sản kỹ thuật số đại diện cho tác phẩm sáng tạo vật lý; kỹ thuật số; tài sản trí tuệ bao gồm âm nhạc, nghệ thuật kỹ thuật số, trò chơi, ảnh gif, video clip,... “*Non-Fungible*” - Không thể thay thế, trong NFT có nghĩa là mỗi mã thông báo không thể trao đổi với một mã thông báo khác, làm cho mỗi mã thông báo trở thành một thực thể duy nhất đại diện cho một đối tượng cụ thể. Các mã thông báo này bao gồm thông tin kỹ thuật số dưới dạng phương tiện (nhạc, video, hình ảnh) mà giá trị của chúng có thể được tính bằng tiền điện tử. Các NFT là một phần của chuỗi khối Ethereum nói riêng nhưng khác với các đồng tiền Ethereum có thể thay thế được, nghĩa là có thể trao đổi với các loại tài sản tương tự.

Mã thông báo không thể thay thế (NFT) là một loại tiền điện tử được bắt nguồn từ hợp đồng thông minh của Ethereum. NFT khác với tiền điện tử cổ điển chẳng hạn như Bitcoin ở chỗ các tính năng bên trong của nó, Bitcoin là một đồng tiền tiêu chuẩn trong đó tất cả các đồng tiền đều tương đương và không thể phân biệt

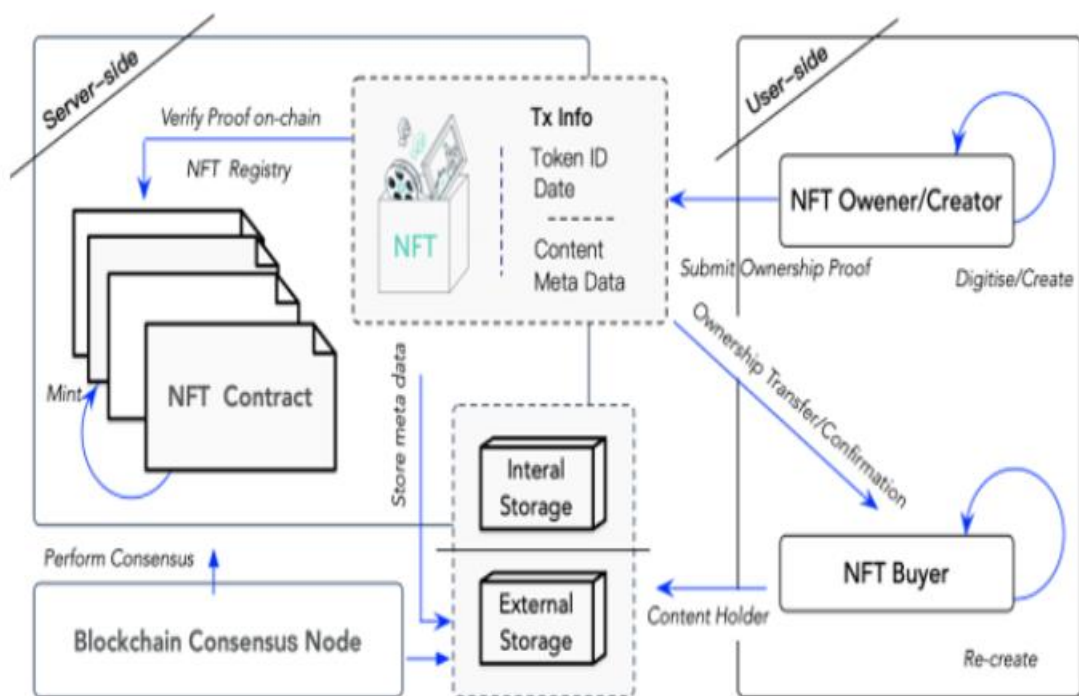


được. Ngược lại, NFT là duy nhất không thể trao đổi (tương đương, không thể thay thế), làm cho nó phù hợp để xác định một cái gì đó hoặc một ai đó theo một cách độc đáo. Cụ thể, bằng cách sử dụng NFT trên các hợp đồng thông minh, người sáng tạo có thể dễ dàng chứng minh sự tồn tại và quyền sở hữu tài sản kỹ thuật số dưới dạng video, hình ảnh, tác phẩm nghệ thuật, sự kiện vé,... Hơn nữa, người sáng tạo cũng có thể kiếm được tiền bản quyền mỗi lần giao dịch thành công trên bất kỳ thị trường NFT nào hoặc bằng cách trao đổi ngang hàng. Toàn bộ lịch sử khả năng giao dịch, thanh khoản và khả năng tương tác thuận tiện cho phép NFT trở thành một giải pháp bảo vệ quyền sở hữu trí tuệ đầy hứa hẹn. Nó đảm bảo tốt giá bán của các sản phẩm liên quan đến sở hữu trí tuệ này mà dường như không thể tưởng tượng được đối với tài sản ảo không thể thay thế.

Trong những năm gần đây, NFT đã thu hút được sự chú ý đáng kể từ cả cộng đồng công nghiệp và khoa học. Mặc dù NFT có tác động tiềm năng to lớn đối với nền tảng thị trường phi tập trung hiện tại và cơ hội kinh doanh trong tương lai, các công nghệ NFT vẫn còn trong giai đoạn đang phát triển. Một số thách thức tiềm năng cần được giải quyết cẩn thận, trong khi một số cơ hội hứa hẹn cần được nêu nổi bật.

### **1.2.3. Giao thức NFT**

Việc thiết lập NFT yêu cầu một sổ cái phân tán cơ bản cho các bản ghi, cùng với các giao dịch có thể trao đổi để giao dịch trong mạng ngang hàng. Sổ cái phân tán là một loại cơ sở dữ liệu đặc biệt lưu trữ dữ liệu NFT. Cụ thể, giả định rằng sổ cái có bảo mật cơ bản tính nhất quán, tính đầy đủ và tính sẵn sàng. Ngoài ra, một hệ thống NFT còn bao gồm hai vai trò khác: chủ sở hữu NFT và người mua NFT. Hình 1.7 cung cấp giao thức chi tiết như sau.



Hình 1.7: Sơ đồ hệ thống NFT

- **Số hóa NFT:** Chủ sở hữu NFT kiểm tra xem tệp, tiêu đề, mô tả có hoàn toàn chính xác. Sau đó, họ số hóa dữ liệu thô thành một định dạng thích hợp.
- **Lưu trữ NFT:** Chủ sở hữu NFT lưu trữ dữ liệu thô vào cơ sở dữ liệu bên ngoài bên ngoài chuỗi khối. Lưu ý rằng, người dùng cũng được phép lưu trữ dữ liệu thô bên trong một chuỗi khối, mặc dù hoạt động này tiêu tốn gas.
- **Ký NFT:** Chủ sở hữu NFT ký một giao dịch, bao gồm cả hàm băm của NFT dữ liệu, sau đó gửi giao dịch đến một hợp đồng thông minh.
- **Đúc tiền & Thương mại NFT:** Sau khi hợp đồng thông minh nhận được giao dịch với dữ liệu NFT, quá trình đúc và giao dịch bắt đầu. Cơ chế chính đằng sau NFT là logic của Tiêu chuẩn mã thông báo
- **Xác nhận NFT:** Sau khi giao dịch được xác nhận, quá trình đúc hoàn thành. Bằng cách tiếp cận này, NFT sẽ liên kết mãi mãi với một chuỗi khối duy nhất địa chỉ như bằng chứng kiên trì của họ.

Trong một hệ thống chuỗi khối, mỗi khối có khả năng giới hạn. Khi công suất trong một khối trở nên đầy, các giao dịch khác sẽ đi vào một khối trong tương lai được liên kết với khối dữ liệu ban đầu. Cuối cùng, tất cả các khối liên kết đã tạo ra một lịch sử lâu dài mà vẫn còn vĩnh viễn. Về bản chất, hệ thống NFT là một hệ thống dựa trên chuỗi khối đăng ký. Bất cứ khi nào một NFT được đúc hoặc bán, một

giao dịch mới là bắt buộc để gửi đề gọi hợp đồng thông minh. Sau khi giao dịch được xác nhận, NFT siêu dữ liệu và chi tiết quyền sở hữu được thêm vào một

khởi mới, do đó đảm bảo rằng lịch sử của NFT không thay đổi và quyền sở hữu được giữ nguyên.

#### 1.2.4. Tiêu chuẩn về Token

Các tiêu chuẩn mã thông báo liên quan đến NFT, bao gồm ERC-20, ERC-721 và ERC-1155 được trình bày Thuật toán 1. Các tiêu chuẩn này có một tác động lớn đến các kế hoạch NFT đang diễn ra. Thuận

---

### Thuật toán 1: Giao diện chuẩn NFT (với các chức năng được chọn)

---

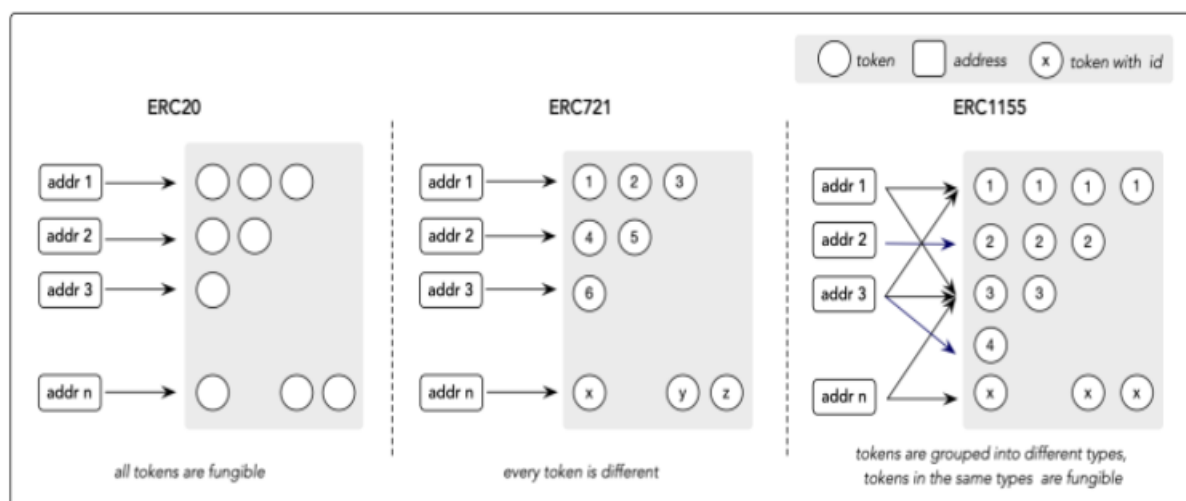
```
interface ERC721 {  
function ownerOf(uint256 tokenId) external view returns  
(address);  
function transferFrom(address from, address to, uint256  
tokenId)  
external payable; ...}  
interface ERC1155 {  
function balanceOf(address owner, uint256 id) external view  
returns  
(address);  
function balanceOfBatch(address calldata owners, uint256  
calldata ids) external view returns (uint256 memory);  
function transferFrom(address from, address to, uint256 id,  
uint256  
quantity) external payable; ...}
```

---

Tiêu chuẩn mã thông báo phổ biến nhất đến từ ERC-20, nó giới thiệu các khái niệm về các mã thông báo có thể thay thế được có thể được phát hành trên Ethereum sau khi thỏa mãn các yêu cầu. Tiêu chuẩn làm cho các mã thông báo giống như một mã thông báo khác (cả về loại và giá trị). Một mã thông báo tùy ý luôn bằng tất cả các mã khác mã thông báo. Rất nhiều chuỗi công khai và các Dapp dựa trên chuỗi khối khác nhau đạt được đủ kinh phí ban đầu theo cách này. Ngược lại, ERC-721 giới thiệu tiêu chuẩn mã thông báo không thể thay thế khác với mã thông báo có thể thay thế, loại này mã thông báo là duy nhất có thể được phân biệt với mã thông báo khác. Cụ thể, mọi NFT đều có một biến *uint256* được gọi là *tokenId* và cặp địa chỉ hợp đồng và *uint256 tokenId* là duy nhất trên toàn

cầu. Hơn nữa, *tokenId* có thể được sử dụng như một đầu vào để tạo nhận dạng đặc biệt, chẳng hạn như hình ảnh nhân vật hoạt hình.

Một tiêu chuẩn khác ERC-1155 (Tiêu chuẩn đa mã thông báo) mở rộng đại diện của cả mã thông báo có thể thay thế và không thể thay thế. Nó cung cấp một giao diện mà có thể đại diện cho bất kỳ số lượng mã thông báo nào. Trong các tiêu chuẩn trước, mọi *tokenId* trong hợp đồng chỉ chứa một loại mã thông báo duy nhất. Chẳng hạn, ERC-20 làm cho mỗi loại mã thông báo được triển khai trong các hợp đồng riêng biệt. Đồng thời, ERC-721 triển khai nhóm của các mã thông báo không thể thay thế trong một hợp đồng có cùng cấu hình. Ngược lại, ERC-1155 mở rộng chức năng của *tokenId*, trong đó mỗi người trong số họ có thể độc lập đại diện cho các loại mã thông báo có thể định cấu hình khác nhau. Trường có thể chứa thông tin tùy chỉnh của nó, chẳng hạn như siêu dữ liệu, thời gian khóa, ngày, nguồn cung cấp, hoặc bất kỳ thuộc tính nào khác. Hình 1.8 cung cấp một minh họa để hiển thị cấu trúc và sự khác biệt nói trên.

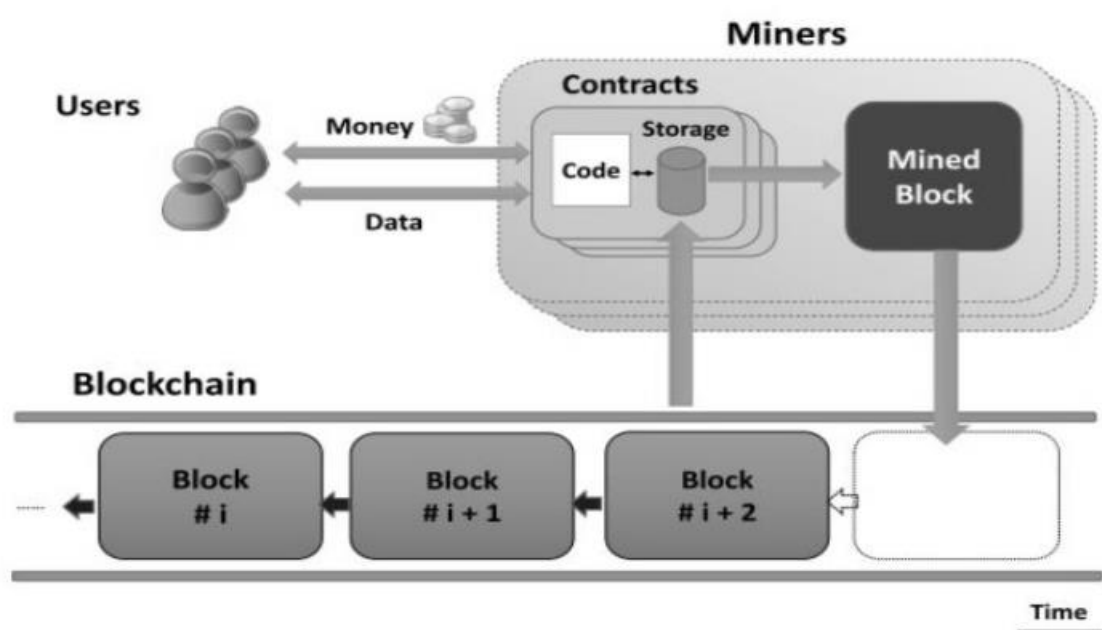


Hình 1.8: Tiêu chuẩn Token của NFT

### 1.2.5. Smart Contract

Hợp đồng thông minh là mã thực thi chạy trên chuỗi khối để tạo điều kiện thuận lợi, thực hiện và thực thi các điều khoản của một thỏa thuận. Mục đích chính của hợp đồng thông minh là tự động thực hiện các điều khoản của một thỏa thuận khi các điều kiện quy định được đáp ứng. Do đó, hợp đồng thông minh với mức phí thấp khi giao dịch so với các hệ thống truyền thống yêu cầu bên thứ ba đáng tin cậy thực thi và thực hiện các điều khoản của một thỏa thuận. Ý tưởng về hợp đồng thông minh đến từ Szabo vào năm 1994. Tuy nhiên, ý tưởng này đã không được đưa ra cho đến khi công nghệ chuỗi khối xuất hiện. Hợp đồng thông minh

có thể được coi là một hệ thống phát hành tài sản kỹ thuật số cho tất cả hoặc một số bên liên quan các bên một khi các quy tắc được xác định trước tùy ý đã được đáp ứng. Chẳng hạn, Alice gửi X tiền tệ đơn vị cho Bob, nếu cô ấy nhận Y đơn vị tiền tệ từ Carl. Có thể phân loại tất cả các định nghĩa thành hai loại, cụ thể là (1) mã hợp đồng thông minh và (2) pháp lý thông minh hợp đồng. Mã hợp đồng thông minh có nghĩa là “mã được lưu trữ, xác minh và thực thi trên chuỗi khối”. Khả năng của hợp đồng thông minh này phụ thuộc hoàn toàn vào ngôn ngữ lập trình được sử dụng để thể hiện hợp đồng và các tính năng của blockchain. Hợp đồng pháp lý thông minh có nghĩa là mã để hợp đồng pháp lý hoàn chỉnh hoặc thay thế. Khả năng của hợp đồng thông minh này không phụ thuộc vào công nghệ, mà thay vào đó là các thể chế pháp lý, chính trị và kinh doanh.



Hình 1.9: Hệ thống hợp đồng thông minh

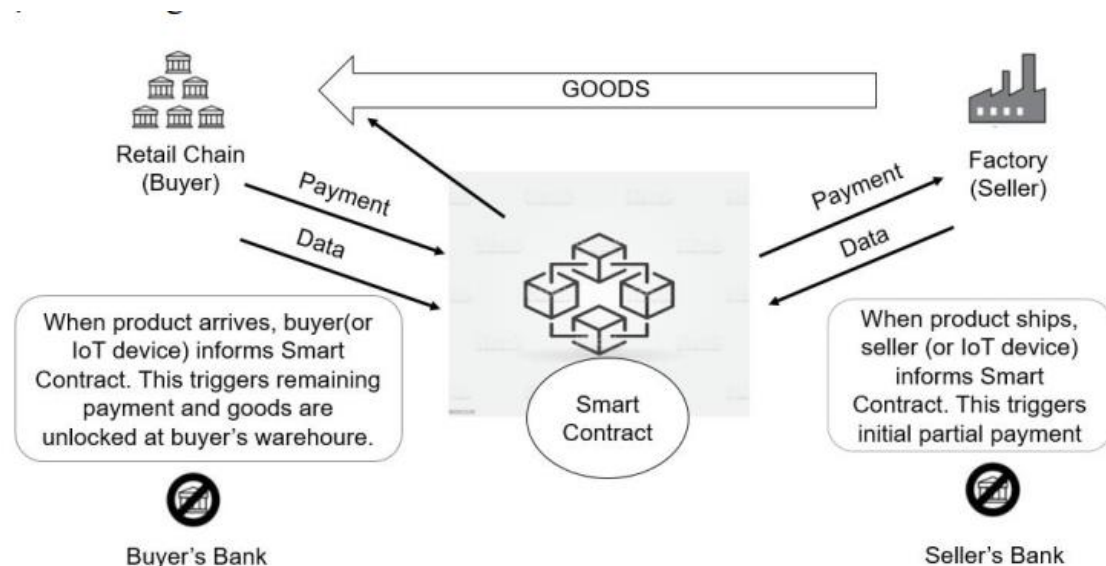
Hợp đồng thông minh có sổ dư tài khoản, bộ nhớ riêng và mã thực thi. Hợp đồng trạng thái bao gồm lưu trữ và sổ dư của hợp đồng. Trạng thái được lưu trữ trên blockchain và nó được cập nhật mỗi khi hợp đồng được gọi. Hình 1.9 mô tả hệ thống hợp đồng thông minh, mỗi hợp đồng sẽ được gán cho một địa chỉ duy nhất là 20 byte. Sau khi hợp đồng được triển khai thành chuỗi khối, mã hợp đồng không thể thay đổi. Để chạy một hợp đồng, người dùng chỉ cần gửi một giao dịch đến địa chỉ của hợp đồng. Giao dịch này sau đó sẽ được thực hiện theo mọi sự đồng thuận nút (được gọi là công cụ khai thác), trong mạng để đạt được sự đồng thuận về đầu ra của nó. Trạng thái của hợp đồng sẽ sau đó được cập nhật cho phù hợp. Hợp đồng có thể dựa trên giao dịch mà nó nhận được; đọc, ghi vào lưu trữ riêng, lưu trữ tiền vào sổ dư tài khoản; gửi, nhận tin nhắn hoặc tiền từ người dùng hoặc thậm chí tạo hợp đồng mới. Có hai loại hợp đồng thông minh, đó là (1) hợp

đồng thông minh xác định và (2) không xác định. Một hợp đồng thông minh xác định là một hợp đồng thông minh khi nó được chạy, nó không yêu cầu bất kỳ thông tin nào từ bên ngoài (từ bên ngoài chuỗi khối). Hợp đồng thông minh không xác định là một hợp đồng phụ thuộc vào thông tin (nguồn cấp dữ liệu) từ một bên ngoài. Ví dụ: một hợp đồng yêu cầu thông tin thời tiết hiện tại được chạy, mà không có sẵn trên blockchain.

### **1.3. Ứng dụng NFT trong thương mại điện tử**

Khi việc sử dụng blockchain trong Giao dịch thương mại được giữ lại, tất cả các bên liên quan có thể tiết kiệm thời gian và nguồn lực bằng cách loại bỏ nhu cầu xử lý thủ công và đối sánh dữ liệu mà họ thực hiện ngày hôm nay và cho phép họ tập trung vào các đề xuất chẳng hạn như tạo ra sản phẩm tốt hơn, có thể quan trọng đối với doanh nghiệp tham gia vào thương mại trong nước và quốc tế. Hình 1.10 mô tả chi tiết các bên tham gia trong giao dịch thương mại điện tử dựa trên Blockchain. Với khả năng hiển thị thời gian thực về các sự kiện dọc theo chuỗi cung ứng, các yếu tố kích hoạt tài chính có thể được xác định sớm hơn. Điều này có nghĩa là tiền có thể được giải phóng nhanh hơn nhiều (giữa người mua và người bán, cũng như với ngân hàng như một phần của thỏa thuận bao thanh toán). Ngoài ra, Blockchain cho phép khả năng của các tác nhân phi ngân hàng (vận chuyển hàng hóa, đại lý hải quan,...) cập nhật vào hệ thống ngay lập tức sau khi giao dịch được hoàn tất.

Giao dịch thương mại đến các giao dịch tài chính, cả trong nước và quốc tế, liên quan đến tài chính các khoản thu thương mại toàn cầu. Giao dịch thương mại là một chức năng kinh doanh cốt lõi cho tất cả các ngân hàng toàn cầu, đặc biệt là ngân hàng cấp 1. Với tầm quan trọng của nó, nó vẫn còn tụt hậu trong ứng dụng công nghệ của nó và vẫn sử dụng các quy trình thủ công cho các luồng tài liệu làm trung tâm. Điều này dẫn đến sự gián đoạn trong các chu kỳ kinh doanh và sự thiếu minh bạch sẽ khiến mở cửa cho tội phạm tài chính. Chuỗi cung ứng giữa nhiều bên rất phức tạp, phân tán, và thiếu sự tin tưởng, do đó họ rất chậm và cần nhiều bên thứ ba như ngân hàng và thanh toán bù trừ cho phép cung ứng thương mại lưu thông.



*Hình 1.10: Mối liên hệ giữa chuỗi bán lẻ, ngân hàng và bên cung ứng trong giao dịch thương mại áp dụng Block Chain*

Hiện nay, blockchain đã và đang được áp dụng trong một số lĩnh vực như thanh toán chạm (quẹt thẻ), ví điện tử, thanh toán trong các nền tảng ứng dụng (VinID; Shopee,...) hay thanh toán bằng QR Code. Khi mua sắm online/offline và quẹt thẻ, một dãy nhị phân (chứa thông tin về thẻ của người dùng) phải đi qua 1 chuỗi các công ty, trong đó, có những hệ thống đã lạc hậu và thiếu tính cập nhật và mất một khoảng thời gian trễ để việc thanh toán được xác nhận. Với ứng dụng công nghệ blockchain, các bên có thể không cần tới quá trình thanh toán này vì việc chi trả và thanh toán sẽ đồng thời xảy ra bằng cơ chế hoạt động của sổ cái phân tán.

Trong lĩnh vực truy xuất nguồn gốc và mã QR, công nghệ Blockchain đã được áp dụng lên một số hàng hóa nông sản tại Việt Nam như vải, nhãn, đào và nhiều sản phẩm khác trong việc gán mã hệ thống của blockchain (hash code) lên tất cả các công đoạn của chuỗi liên kết cho sản phẩm mang mã QR. Điều này cho phép hệ thống xác định chính xác trạng thái của sản phẩm trong từng thời điểm như hàng đã đóng gói, hàng đã chuyển, hàng đã bán,... Ứng dụng công nghệ Blockchain cho phép người tiêu thụ và nhà quản lý nắm được toàn bộ quy trình từ sản xuất ra sản phẩm đến khi sản phẩm được bán cho người tiêu thụ. Nếu những dữ liệu sản xuất được cập nhật trung thực (đó là lý do vì sao cần sử dụng IoT) thì bức tranh sản xuất sẽ hiện ra chính xác. Thông qua đó, người sản xuất biết rõ trạng thái sản xuất của mình để điều chỉnh, nâng cấp và phát triển cũng như làm cho việc giao dịch với người tiêu dùng trở nên minh bạch, nhanh chóng và hiệu quả hơn.

Tại Việt Nam, Ngân hàng TNHH Một thành viên HSCB Việt Nam (HSCB Việt Nam) và Ngân hàng TMCP Ngoại thương Việt Nam (Vietcombank) vừa thông

báo đã đồng thực hiện thành công một giao dịch bằng thư tín dụng trong nước (LC) bằng tiền đồng trên nền tảng blockchain đầu tiên tại Việt Nam.

Giao dịch được thực hiện trên nền tảng Contour, trên cơ sở công nghệ blockchain Corda của R3, là một phần của giai đoạn thử nghiệm Beta của Contour.

Hiện nay NFT có thể được ứng dụng đa dạng trong nhiều lĩnh vực, trong nghệ thuật (âm nhạc, video, tranh ảnh...), trò chơi điện tử (giao diện, vật phẩm game)... với bất cứ sản phẩm có thể tồn tại dưới dạng kỹ thuật số.

#### *Nghệ thuật số*

Nghệ thuật kỹ thuật số là một trường hợp sử dụng phổ biến cho NFT. Các cuộc đấu giá NFT nổi tiếng liên quan đến nghệ thuật kỹ thuật số đã nhận được sự quan tâm đáng kể của công chúng. Tác phẩm có tựa đề “The merge” của nghệ sĩ Pak là NFT đắt nhất với đấu giá là 91,8 triệu đô la Mỹ và “Everydays: the First 5000 Days” của nghệ sĩ Mike Winkelmann (được biết đến với tên chuyên nghiệp là Beeple) đắt thứ hai với giá đô la Mỹ 69,3 triệu vào năm 2021.

#### *Trò chơi*

NFT đóng một vai trò trong cả trò chơi điện tử truyền thống cũng như trò chơi điện tử dựa trên chuỗi khối. Mặc dù trước đây, chúng thường đại diện cho các bổ sung thẩm mỹ có thể được gán cho một người chơi riêng lẻ nhưng chúng thường là cốt lõi của trò chơi blockchain.

NFT có thể đại diện cho tài sản trong trò chơi, chẳng hạn như các lô đất kỹ thuật số. Một số nhà bình luận mô tả những thứ này được kiểm soát "bởi người dùng" thay vì nhà phát triển trò chơi nếu chúng có thể được giao dịch trên thị trường của bên thứ ba mà không cần sự cho phép của nhà phát triển trò chơi. Tuy nhiên, sự đón nhận của họ từ các nhà phát triển trò chơi nói chung là trái chiều, với một số người như Ubisoft nắm lấy công nghệ nhưng Valve và Microsoft chính thức cấm họ.

CryptoKitties là một trò chơi trực tuyến chuỗi khối thành công ban đầu, trong đó người chơi nhận nuôi và buôn bán mèo ảo. Việc kiếm tiền từ NFT trong trò chơi đã huy động được khoản đầu tư 12,5 triệu đô la, với một số chú mèo con được bán với giá hơn 100.000 đô la mỗi con. Sau thành công của nó, CryptoKitties đã được thêm vào tiêu chuẩn ERC-721, được tạo vào tháng 1 năm 2018 (và được hoàn thiện vào tháng 6).

#### *Âm nhạc và phim*

Trong ngành công nghiệp điện ảnh, NFT quan trọng nhất cung cấp khả năng mã hóa các cảnh phim và bán chúng dưới dạng đồ sưu tầm dưới dạng NFT. Trong ngành công nghiệp âm nhạc, các nghệ sĩ có thể giành nhiều quyền kiểm soát hơn đối với tác phẩm nghệ thuật của họ mà không bị bên thứ ba can thiệp bằng cách sử dụng NFT. Các nghệ sĩ tham gia vào một trong hoặc cả hai phân khúc của ngành công nghiệp giải trí có thể sử dụng NFT để đảm bảo rằng họ sẽ nhận được tiền bản quyền, để giảm thiểu cả tác động tài chính cũng như mức độ liên quan của các bản sao vi phạm bản quyền tác phẩm nghệ thuật của họ cũng như để tham gia vào loại hình nghệ thuật của họ mà không bị ảnh hưởng bởi các hãng nhạc,



hãng phim hay bất kỳ bên thứ ba nào khác. Cho đến nay, NFT thường được sử dụng trong cả ngành công nghiệp âm nhạc cũng như điện ảnh. Vào tháng 3 năm 2021, bộ phim tài liệu năm 2015 của Adam Benzine Claude Lanzmann: Spectre of the Shoah đã trở thành phim tài liệu và phim điện ảnh đầu tiên được bán đấu giá dưới dạng NFT.

#### **1.4. Đánh giá về bảo mật NFT**

Hệ thống NFT là một công nghệ kết hợp bao gồm chuỗi khối, lưu trữ và ứng dụng Web. Việc đánh giá bảo mật trên hệ thống NFT là một thách thức vì mỗi thành phần có thể trở thành một giao diện tấn công khiến toàn bộ hệ thống thực sự dễ bị kẻ tấn công tấn công. Do đó, áp dụng đánh giá rủi ro và mối đe dọa mô hình STRIDE, bao gồm tất cả các khía cạnh bảo mật của hệ thống: tính xác thực, tính toàn vẹn, tính không thể từ chối, tính khả dụng và kiểm soát truy cập. Việc điều tra các vấn đề bảo mật tiềm ẩn và đề xuất một số biện pháp bảo vệ tương ứng để giải quyết các vấn đề này đã được trình bày trong Bảng 1.

– *Spoofing*: Spoofing là khả năng mạo danh một thực thể khác (ví dụ: một người hoặc máy tính khác) trên hệ thống, tương ứng với tính xác thực. Khi người dùng tương tác để đúc hoặc bán NFT, kẻ tấn công độc hại có thể khai thác các lỗ hổng xác thực hoặc đánh cắp khóa riêng của người dùng để chuyển quyền sở hữu NFT một cách bất hợp pháp. Do đó, nên xác minh chính thức cho hợp đồng thông minh NFT và sử dụng ví lạnh để ngăn rò rỉ khóa riêng.

– *Tampering*: Tampering đề cập đến việc sửa đổi độc hại dữ liệu NFT, vi phạm tính toàn vẹn. Giả sử rằng chuỗi khối là một cường tráng sổ cái giao dịch công khai và một thuật toán băm là khả năng chống lại hình ảnh trước và khả năng chống lại hình ảnh thứ hai. Siêu dữ liệu và quyền sở hữu của NFT không thể bị sửa đổi một cách ác ý sau khi giao dịch được xác nhận. Tuy nhiên, dữ liệu được lưu trữ bên ngoài chuỗi khối có thể bị thao túng. Do đó, người dùng nên gửi cả dữ liệu băm cũng như dữ liệu gốc cho người mua NFT khi giao dịch/trao đổi các tài sản liên quan đến NFT.

– *Repudiation*: Repudiation đề cập đến tình huống mà tác giả của một tuyên bố không thể tranh chấp, liên quan đến tài sản bảo đảm của tính không thể từ chối. Đặc biệt, không thể phủ nhận việc một người dùng gửi NFT cho một người dùng khác. Điều này được đảm bảo bởi tính bảo mật của chuỗi khối và thuộc tính không thể sửa chữa của sơ đồ chữ ký. Tuy nhiên, dữ liệu băm có thể bị giả mạo bởi kẻ tấn công nguy hiểm hoặc dữ liệu băm có thể liên kết với mã hóa của kẻ tấn công. Địa chỉ. Vì vậy, việc sử dụng hợp đồng nhiều chữ ký có thể giải quyết phần nào vấn đề này vì mỗi ràng buộc phải được xác nhận bởi nhiều bên tham gia.

– *Information Disclosure*: Rò rỉ thông tin xảy ra khi thông tin bị lộ cho người dùng trái phép, vi phạm tính bảo mật. Trong hệ thống NFT, thông tin trạng thái và mã hướng dẫn trong hợp đồng thông minh hoàn toàn minh bạch và bất kỳ trạng thái nào cũng như những thay đổi của nó đều có thể truy cập công khai bởi bất kỳ người quan sát nào. Ngay cả khi người dùng chỉ đặt hàm băm NFT vào chuỗi khối, những kẻ tấn công độc hại có thể dễ dàng khai thác khả năng liên kết của hàm băm và giao dịch. Do đó, các nhà phát triển NFT nên sử dụng hợp đồng

thông minh bảo vệ quyền riêng tư thay vì hợp đồng thông minh đơn giản để bảo vệ quyền riêng tư của người dùng.

– *Denial of Service (DoS)*: Tấn công DoS là một kiểu tấn công mạng trong đó kẻ tấn công độc hại nhằm mục đích làm cho máy chủ không khả dụng với người dùng dự kiến bằng cách làm gián đoạn các chức năng bình thường. DoS vi phạm tính khả dụng và phá vỡ dịch vụ NFT, dịch vụ này thực sự có thể được sử dụng bởi người dùng trái phép. May mắn thay, chuỗi khối đảm bảo tính sẵn sàng cao cho các hoạt động của người dùng. Người dùng hợp pháp có thể sử dụng thông tin cần thiết khi cần và sẽ không bị mất tài nguyên dữ liệu do lỗi ngẫu nhiên. Tuy nhiên, DoS cũng có thể được sử dụng để tấn công các ứng dụng web tập trung hoặc dữ liệu thô bên ngoài chuỗi khối, dẫn đến tấn công từ chối dịch vụ đối với dịch vụ NFT. Gần đây, một kiến trúc blockchain lai mới với thuật toán đồng thuận yếu đã được đề xuất, theo đó kiến trúc này giải quyết các vấn đề về tính khả dụng bằng hai thuật toán.

– *Elevation of Privilege*: Nâng cao đặc quyền là một tài sản có liên quan đến ủy quyền. Trong loại mối đe dọa này, kẻ tấn công có thể giành được các quyền vượt quá những quyền được cấp ban đầu. Trong hệ thống NFT, quyền bán được quản lý bởi một hợp đồng thông minh. Một lần nữa, một hợp đồng thông minh được thiết kế kém có thể khiến NFT mất đi những đặc tính như vậy.

*Bảng 1: Các vấn đề bảo mật tiềm ẩn và giải pháp tương ứng của NFT*

STRIDE	Vấn đề về bảo mật	Giải pháp
Spoofing (Authenticity)	<ul style="list-style-type: none"> <li>• Kẻ tấn công có thể khai thác lỗ hổng xác thực</li> <li>• Kẻ tấn công có thể đánh cắp một khóa riêng của người dùng</li> </ul>	<ul style="list-style-type: none"> <li>• Một xác minh chính thức về hợp đồng thông minh.</li> <li>• Sử dụng ví lạnh để ngăn rò rỉ khóa cá nhân</li> </ul>
Tampering (Integrity)	<ul style="list-style-type: none"> <li>• Dữ liệu được lưu trữ bên ngoài chuỗi khối có thể bị thao túng.</li> </ul>	<ul style="list-style-type: none"> <li>• Gửi cả dữ liệu gốc và dữ liệu băm cho người mua NFT khi giao dịch NFT</li> </ul>
Repudiation (Non repudiability)	<ul style="list-style-type: none"> <li>• Dữ liệu băm có thể liên kết với địa chỉ của kẻ tấn công.</li> </ul>	<ul style="list-style-type: none"> <li>• Sử dụng một phần hợp đồng nhiều chữ ký.</li> </ul>
Information disclosure (Confidentiality)	<ul style="list-style-type: none"> <li>• Kẻ tấn công có thể dễ dàng khai thác hàm băm và giao dịch để liên kết một người mua hoặc người bán NFT cụ thể.</li> </ul>	<ul style="list-style-type: none"> <li>• Sử dụng hợp đồng thông minh bảo vệ quyền riêng tư thay vì</li> <li>• hợp đồng thông minh để bảo vệ quyền riêng tư của người dùng.</li> </ul>

<b>Denial of service</b> (Availability)	<ul style="list-style-type: none"> <li>• Dữ liệu NFT có thể không khả dụng nếu nội dung được lưu trữ bên ngoài chuỗi khối.</li> </ul>	<ul style="list-style-type: none"> <li>• Sử dụng kiến trúc chuỗi khối lai với thuật toán đồng thuận yếu.</li> </ul>
<b>Elevation of privilege</b> (Authorization)	<ul style="list-style-type: none"> <li>• Hợp đồng thông minh được thiết kế kém có thể khiến NFT thua lỗ những tính chất như vậy.</li> </ul>	<ul style="list-style-type: none"> <li>• Xác minh chính thức về hợp đồng thông minh.</li> </ul>

## CHƯƠNG 2: Giải pháp phát triển game thương mại dựa trên công nghệ NFT

### 2.1. Công nghệ Polygon

#### 2.1.1. Tổng quan về công nghệ Polygon

Polygon trước đây được gọi là mạng MATIC, là một giải pháp khả năng mở rộng liên chuỗi cung cấp một cơ sở hạ tầng để tạo mạng Blockchain mà có thể giao tiếp với nhau. Polygon mang lại khả năng thích ứng và khả năng mở rộng của chuỗi cùng với tính bảo mật, tính thanh khoản và khả năng tương tác. Nó sẽ phân phối vô số trao đổi ngoài chuỗi cùng nhau thành một thương mại đơn độc, trong khi người dùng khác sẽ chạy trên mạng Ethereum để tăng tốc giao dịch. Nó cung cấp hợp đồng thông minh dưới dạng PoS (Proof-of-Stake). Tuy nhiên, việc áp dụng nhanh Ethereum dẫn đến chi phí rất cao, với phí trao đổi thường xuyên chi phí nhiều hơn số tiền chuyển nhượng. Trong những trường hợp như vậy, Polygon được sử dụng để giải quyết các vấn đề. Máy khách Polygon sử dụng MATIC Sidechain để thực thi và hợp tác với các ứng dụng phi tập trung dựa trên Ethereum khác nhau, tạo ra nhiều MATIC rẻ hơn và nhanh hơn các mạng khác. Hệ thống dựa vào các nhà phát triển để lắp ráp chuỗi bên của riêng họ hoặc để mở rộng quy mô ứng dụng của họ sử dụng SDK Polygon (phát triển phần mềm kit) ngăn xếp và mạng để cung cấp cho khách hàng của họ một trải nghiệm người dùng cuối tốt hơn. Điều đáng chú ý là SDK Polygon tương thích với nhiều loại ngôn ngữ lập trình hợp đồng thông minh hiện có, cung cấp tính mô-đun và có thể mở rộng. Các bên liên quan trên Polygon thành công hoạt động giống như công cụ khai thác PoW trên Ethereum. Để phê duyệt và xác nhận trao đổi trên MATIC Sidechain, các bên liên quan phải khóa mã thông báo MATIC. Ngoài ra, họ có thể chọn đủ điều kiện chặn người tạo bằng cách sử dụng mã thông báo bị khóa của họ như quyền biểu quyết của họ để điều chỉnh các quá trình tạo khối trên sidechain. Thông thường, số lượng người tạo khối được giữ thấp vừa phải với lý do có một vài các nhà sản xuất thỏa thuận khối có xu hướng cung cấp thông lượng cao hơn và trao đổi nhanh hơn nhiều định cư. Ví dụ, trung bình, các Ethereum mainchain mất khoảng 20 giây để tạo một khối mới, trong khi MATIC Sidechain sản xuất và giải quyết các khối mới trong vòng một giây.

Polygon là một giải pháp mở rộng quy mô “Lớp 2” đạt được quy mô bằng cách sử dụng các chuỗi bên để tính toán ngoài chuỗi và mạng lưới trình xác thực Proof-of-Stake (PoS) phi tập trung. Polygon cố gắng giải quyết các vấn đề về khả năng mở rộng và khả năng sử dụng trong khi không ảnh hưởng đến việc phân cấp và tận dụng cộng đồng nhà phát triển và hệ sinh thái hiện có. Nó nhằm mục đích cải thiện các nền tảng hiện có bằng cách cung cấp khả năng mở rộng và trải nghiệm người dùng vượt trội cho Dapps và các chức năng của người dùng. Nó là một giải pháp mở rộng quy mô cho các chuỗi khối công khai. Polygon PoS hỗ trợ tất cả các công cụ Ethereum hiện có cùng với các giao dịch nhanh hơn và rẻ hơn.

Các tính năng và điểm nổi bật của Polygon:

- *Khả năng mở rộng*: Giao dịch nhanh, chi phí thấp và an toàn trên Polygon sidechains với tính hữu hạn đạt được trên chuỗi chính và Ethereum là chuỗi cơ sở *Lớp 1* tương thích đầu tiên.
- *Thông lượng cao*: Đạt được tới 10.000 TPS trên một sidechain duy nhất trên testnet nội bộ; nhiều chuỗi sẽ được thêm vào để chia tỷ lệ theo chiều ngang.

– *Trải nghiệm người dùng*: UX mượt mà và trừu tượng hóa nhà phát triển từ chuỗi chính đến chuỗi Polygon; SDK và ứng dụng dành cho thiết bị di động gốc có hỗ trợ WalletConnect.

– *Bảo mật*: Bản thân các nhà khai thác chuỗi Polygon cũng là những người đặt cược trong hệ thống PoS.

– *Chuỗi công khai Sidechains*: Polygon sidechains có bản chất công khai (so với các chuỗi Dapp riêng lẻ) và có khả năng hỗ trợ nhiều giao thức. Hệ thống Polygon được kiến trúc một cách có chặt chẽ để hỗ trợ các chuyển đổi trạng thái tùy ý trên Polygon sidechains và được kích hoạt EVM.

30

### **2.1.2. Phương thức hoạt động Polygon**

Phương thức hoạt động của Polygon có thể được diễn tả như sau: Chuỗi Polygon được xây dựng song song với chuỗi chính Ethereum, nhằm hỗ trợ xử lý giao dịch. Vì vậy, để thực hiện giao dịch, người dùng sẽ gửi tiền điện tử của mình lên Ethereum. Sau đó, thay vì giao dịch trực tiếp trên mạng Ethereum, có thể chuyển sang giao dịch trên chuỗi Polygon để tránh được tình trạng tắc nghẽn do có quá nhiều giao dịch. Lúc này, token trên tài khoản Ethereum đã được xác nhận và đưa lên chuỗi Polygon với lượng tương ứng, sẵn sàng để có thể thực hiện bất cứ giao dịch nào. Chuỗi chính Ethereum sẽ có trách nhiệm ghi nhận lại số dư cuối cùng và thông báo cho người dùng. Quá trình này có thể giúp Ethereum giảm bớt được lượng giao dịch, hạn chế được tình trạng tắc nghẽn; đồng thời cũng có thể giao dịch nhanh chóng hơn.

Người dùng gửi tiền điện tử trong hợp đồng Polygon trên chuỗi chính, hiện tại là Blockchain Ethereum. Sau khi các token đã gửi được xác nhận trên chuỗi chính, các token tương ứng sẽ được đưa lên chuỗi Polygon. Người dùng có thể chuyển token cho bất kỳ ai họ muốn ngay lập tức với mức phí không đáng kể. Chuỗi Polygon có các khối nhanh hơn (khoảng 1 giây hoặc ít hơn). Bằng cách đó, quá trình giao dịch sẽ được thực hiện gần như ngay lập tức. Nếu người dùng muốn, họ có thể rút các token còn lại từ chuỗi chính bằng cách thiết lập bằng chứng về các token còn lại trên hợp đồng gốc trên chuỗi Ethereum.

### **2.1.3. Kiến trúc công nghệ Polygon**

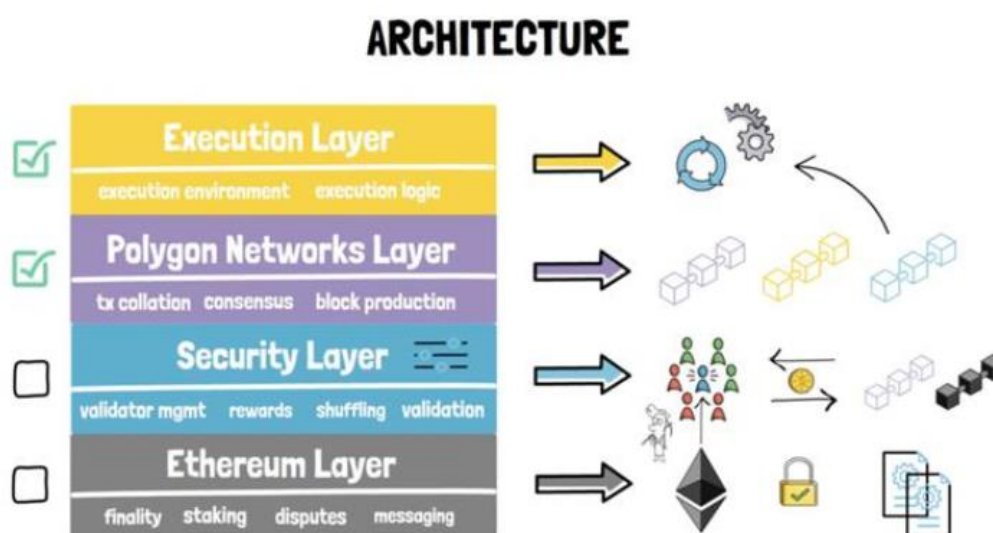
Polygon sở hữu hệ thống bao gồm 4 lớp chính: Lớp Ethereum, lớp bảo mật, lớp mạng Polygon và lớp thực thi.

- *Lớp Ethereum (Lớp tùy chọn)*: Những chuỗi Polygon có thể sử dụng tính năng bảo mật của Ethereum để làm Base Layer cho hệ thống của chúng. Các Layer này được sử dụng như một tập hợp những hợp đồng thông minh tạo ra trên Ethereum nên có thể sử dụng vào các trường hợp như tính toán và kiểm tra Staking, trao đổi, giải quyết những tranh chấp giữa Ethereum và Polygon Chains.

- *Lớp bảo mật (Lớp tùy chọn)*: Tương tự như Ethereum Layer, Security cũng là một Layer không bắt buộc phải có mặt trên Polygon. Đây là Layer có thể cung cấp chức năng “validators as a service” cho phép Polygon Chains sử dụng một tập hợp các trình xác thực có thể kiểm tra định kỳ tính hợp lệ của bất kỳ mạng nào đó trong Polygon chains với khoản phí nhất định. Layer này thường triển khai như một Meta trên nền tảng Blockchain và chạy song song với Ethereum. Hoạt động này được chịu trách nhiệm quản lý xác thực – đăng ký/ hủy đăng ký, phần thưởng, tổ chức lại và xác thực bởi Polygon Chains.

- *Lớp Mạng Polygon (Lớp bắt buộc)*: Đây là một trong những Layer bắt buộc phải có trên Polygon, gồm có hệ thống mạng Blockchain có chủ quyền, mỗi Blockchain sẽ đảm nhận những chức năng nhất định như đối chiếu giao dịch, đồng thuận hoặc sản xuất Block.

- *Lớp thực thi (Lớp bắt buộc)*: Cuối cùng là Layer Execution Layer với vai trò vô cùng quan trọng, chịu trách nhiệm giải thích và thực hiện các giao dịch trong Polygon Chains. Trong Layer này bao gồm môi trường điều hành các Layer con logic điều hành.



Hình 2.1: Mô hình kiến trúc 4 lớp của công nghệ Polygon

#### 2.1.4. Chuỗi Polygon PoS và chuỗi Polygon Plasma

Chuỗi PoS là chuỗi chính của nền tảng, thường được gọi là sidechain Ethereum hay chuỗi PoS Matic. Ngoài ra, chuỗi này bổ sung thêm lớp bảo mật PoS (bằng chứng cổ phần) cho các blockchain khởi chạy trên nền tảng của Polygon. Chuỗi Plasma này có chức năng chính là giúp dễ dàng di chuyển được tài sản số của người dùng giữa chuỗi gốc và chuỗi con.

##### 2.1.4.1. Proof of Stack (PoS)

Bằng chứng cổ phần (PoS) làm cơ sở cho các cơ chế đồng thuận nhất định được sử dụng bởi các chuỗi khối để đạt được sự đồng thuận. Trong bằng chứng công việc (PoW), những người khai thác (miners) chứng minh rằng họ có rủi ro về vốn bằng cách sử dụng năng lượng. Ethereum sử dụng bằng chứng cổ phần, trong đó các trình xác nhận (validator) đặt vốn rõ ràng dưới dạng ETH vào một Hợp đồng thông minh trên Ethereum. Số ETH đã đặt cọc này sau đó đóng vai trò là tài sản thế chấp có thể bị hủy nếu người xác nhận có hành vi không trung thực hoặc không chăm chỉ. Trình xác thực sau đó chịu trách nhiệm kiểm tra xem các khối mới được truyền qua mạng có hợp lệ hay không và đôi lúc tự tạo và truyền các khối mới.

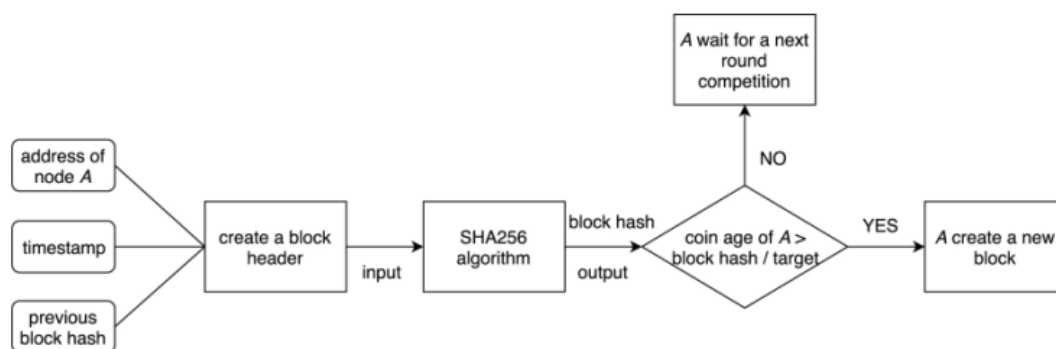
Bằng chứng cổ phần (PoS) đi kèm với một số cải tiến đối với hệ thống bằng chứng công việc:

- Hiệu quả năng lượng tốt hơn: không cần sử dụng nhiều năng lượng cho các tính toán bằng chứng công việc;
- Rào cản gia nhập thấp hơn, giảm yêu cầu phần cứng: không cần phần cứng tốt để có cơ hội tạo khối mới;
- Giảm rủi ro tập trung: bằng chứng cổ phần sẽ dẫn đến nhiều nút bảo vệ mạng hơn;
- Do yêu cầu năng lượng thấp nên ít phát hành ETH hơn để khuyến khích sự tham gia;
- Hình phạt kinh tế cho hành vi sai trái làm cho kẻ tấn công kiểu tấn công 51% tốn kém hơn theo cấp số nhân so với bằng chứng công việc;
- Cộng đồng có thể dùng đến sự phục hồi xã hội của một chuỗi trung thực nếu một cuộc tấn công 51% vượt qua được các biện pháp phòng thủ kinh tế tiền điện tử.

Để giải quyết vấn đề tiêu thụ điện năng tính toán lớn của PoW, các nhà nghiên cứu đã đề xuất thuật toán đồng thuận Proof of Stake (PoS). Quá trình của PoS khác với PoW vì người dùng giao thức PoS không yêu cầu giải bài toán để đạt được sự đồng thuận, mặt khác người dùng chỉ cần sử dụng tiền điện tử làm cổ phần để đạt được sự đồng thuận. Có 2 cách để tham gia đặt cược, luồng thuật toán PoS được minh họa trong Hình 2.2.

(1) Đầu tiên, người dùng có thể cho những người dùng khác vay tiền của họ để tham gia vào nhóm và sau đó chia sẻ lợi nhuận với họ. Tuy nhiên, người dùng sẽ cần tìm một người đáng tin cậy để đặt cược cùng. Một phương pháp khác là tham gia nhóm, mọi người tham gia vào nhóm cụ thể đó sẽ chia lợi nhuận dựa trên số tiền đặt cược.

(2) Người tạo khối mới được chọn từ nhóm người dùng đã đặt cược một lượng tiền điện tử nhất định và không người dùng nào có thể dự đoán trước lượt của khối đó. Số lượng cổ phần mà một người có trong hệ thống sẽ quyết định việc khai thác. Nếu một người khai thác có nhiều cổ phần hơn trong chuỗi khối, cơ hội khai thác nhiều hơn, chẳng hạn nếu cổ phần trong loại tiền điện tử nhất định là 1%, thì người dùng có thể tạo ra tới 1% giao dịch.



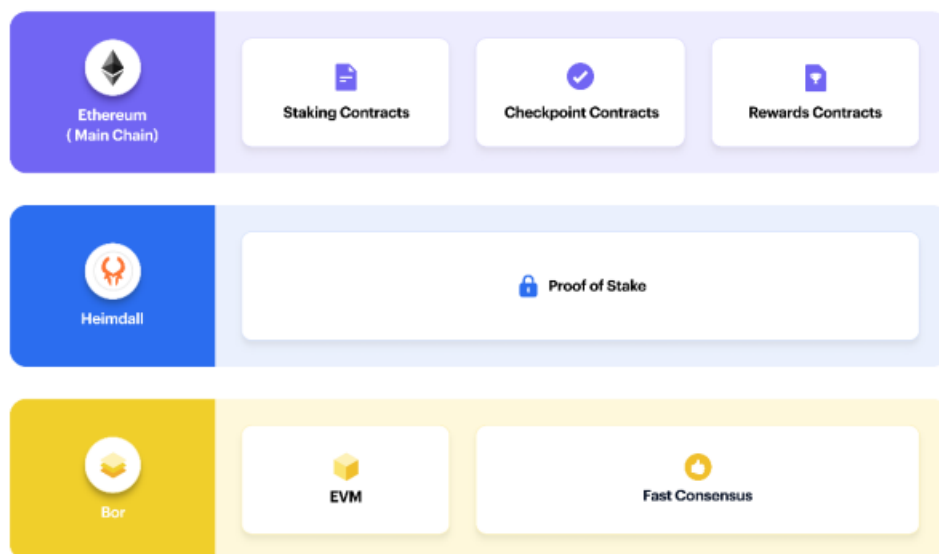
Hình 2. 2: Luồng thuật toán PoS

PoS khuyến khích những người nắm giữ tiền xu tăng thời gian nắm giữ. Chuỗi khối không còn phụ thuộc hoàn toàn vào PoW nhờ vào khái niệm tiền đúc. Điều đó giải quyết hiệu quả vấn đề lãng phí tài nguyên trong PoW. Với giá trị gia tăng trong chuỗi khối, tính bảo mật của chuỗi khối sử dụng PoS được cải thiện. Những kẻ tấn công cần tích lũy một số lượng lớn tiền xu và giữ chúng trong một thời gian dài để tấn công chuỗi khối. Điều này cũng làm tăng đáng kể độ khó của cuộc tấn công. Mặc dù phương pháp này giảm lãng phí năng lượng tính toán, nhưng nó có thể tiềm ẩn nguy cơ độc quyền, dẫn đến xu hướng tập trung hóa hệ thống, đồng thời cho phép những kẻ tấn công độc hại có mục tiêu tấn công rõ ràng, gây rủi ro về bảo mật.

#### 2.1.4.2. Chuỗi Polygon PoS

Polygon PoS có kiến trúc ba lớp:

- *Lớp Ethereum*: một tập hợp các Hợp đồng trên mạng chính Ethereum.
- *Lớp Heimdall*: một tập hợp các nút Heimdall bằng chứng cổ phần chạy song song với mạng chính Ethereum, giám sát tập hợp các hợp đồng đặt cược được triển khai trên mạng chính Ethereum và cam kết các điểm kiểm tra mạng Polygon cho mạng chính Ethereum.
- *Lớp Bor*: một tập hợp các nút Bor tạo khối được xáo trộn bởi các nút Heimdall.



Hình 2. 3: Mô hình kiến trúc mạng Polygon PoS

#### Hợp đồng thông minh Polygon (trên Ethereum)

Polygon duy trì một bộ hợp đồng thông minh trên Ethereum, xử lý những việc sau:

- Quản lý đặt cược cho lớp Proof-of-Stake
- Quản lý ủy quyền bao gồm cổ phiếu xác thực



- Checkpoints/snapshots trạng thái sidechain

*Heimdall (lớp trình xác thực Proof-of-Stake)*

- Heimdall là nút xác thực PoS hoạt động đồng bộ với các hợp đồng đặt cược trên Ethereum để kích hoạt cơ chế PoS trên Polygon. Triển khai điều này bằng cách xây dựng dựa trên công cụ đồng thuận Tendermint với các thay đổi đối với sơ đồ chữ ký và các cấu trúc dữ liệu khác nhau. Nó chịu trách nhiệm xác thực khối, lựa chọn ủy ban sản xuất khối, kiểm tra điểm đại diện của các khối sidechain cho Ethereum trong kiến trúc Polygon và nhiều trách nhiệm khác.

- Lớp Heimdall xử lý việc tổng hợp các khối do Bor tạo ra thành một cây merkle và xuất bản gốc merkle theo định kỳ lên chuỗi gốc. Những xuất bản định kỳ này được gọi là *checkpoints*. Đối với mỗi vài khối trên Bor, một trình xác thực (trên lớp Heimdall):

- Xác thực tất cả các khối kể từ điểm kiểm tra cuối cùng
- Tạo một cây merkle của khối băm
- Xuất bản gốc merkle lên chuỗi chính

- Checkpoints (điểm kiểm tra) rất quan trọng vì hai lý do:

- Cung cấp tính hữu hạn trên Root Chain
- Cung cấp Proof of Burn khi rút tài sản

Một cái nhìn toàn cảnh về quá trình có thể được giải thích như sau:

– Một tập hợp con các trình xác thực đang hoạt động từ nhóm được chọn để đóng vai trò là nhà sản xuất khối trong một khoảng thời gian. Việc Lựa chọn từng nhịp cũng sẽ được ít nhất 2/3 quyền lực nhất trí. Các nhà sản xuất khối này chịu trách nhiệm tạo các khối và phát nó đến mạng còn lại.

– Một điểm kiểm tra bao gồm gốc của tất cả các khối được tạo trong bất kỳ khoảng thời gian nhất định nào. Tất cả các nút xác thực giống nhau và đính kèm chữ ký của họ vào đó.

– Người đề xuất được chọn từ bộ trình xác thực chịu trách nhiệm thu thập tất cả chữ ký cho một điểm kiểm tra cụ thể và cam kết tương tự trên chuỗi chính.

– Trách nhiệm tạo khối và cũng như đề xuất các điểm kiểm tra phụ thuộc rất nhiều vào tỷ lệ cổ phần của người xác thực trong nhóm tổng thể.

*Bor (Lớp sản xuất khối)*

– Bor là lớp sản xuất khối Polygon - thực thể chịu trách nhiệm tổng hợp các giao dịch thành các khối.

– Các nhà sản xuất khối được xáo trộn định kỳ thông qua lựa chọn của ủy ban trên Heimdall trong khoảng thời gian được gọi là span trong Polygon.

Các khối được tạo ra tại nút Bor và sidechain VM tương thích với EVM.

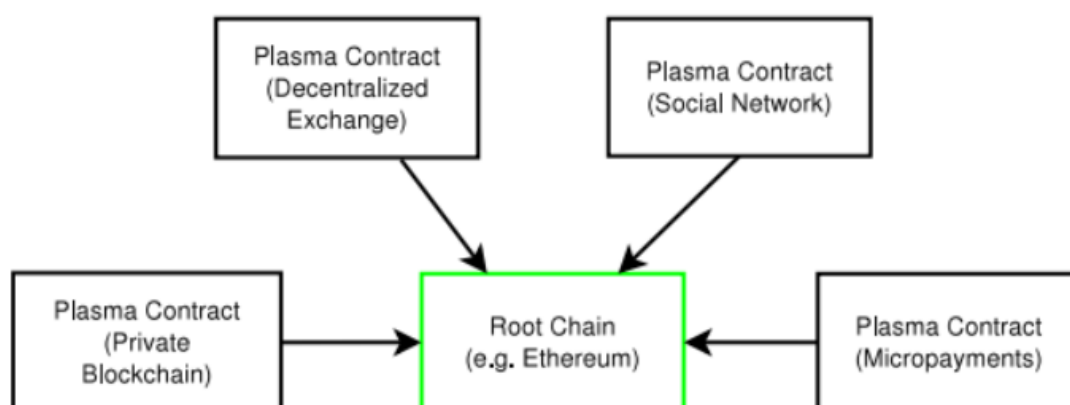
Các khối được tạo trên Bor cũng được xác thực định kỳ bởi các nút

Heimdall và một điểm kiểm tra bao gồm hàm băm cây Merkle của một tập hợp các khối trên Bor được cam kết với Ethereum theo định kỳ.

### 2.1.4.3. Chuỗi Matic Plasma

Plasma là một cách để thực hiện tính toán có thể mở rộng trên chuỗi khối với cấu trúc tạo ra các những khuyến khích về mặt kinh tế để vận hành chuỗi một cách tự chủ và liên tục mà không cần sự quản lý chuyển đổi trạng thái tích cực của người tạo hợp đồng. Bản thân các nút được khuyến khích vận hành chuỗi.

Ngoài ra, khả năng mở rộng đáng kể đạt được bằng cách giảm thiểu số tiền được thể hiện trong một khoản chi tiêu từ hợp đồng thành một bit duy nhất trong bản đồ bit, để một giao dịch và chữ ký đại diện cho một khoản thanh toán được kết hợp với nhiều người tham gia. Những nhà sáng lập của Polygon kết hợp điều này với khung MapReduce để có thể xây dựng khả năng tính toán có thể mở rộng được thực thi bởi các hợp đồng thông minh được liên kết. Cấu trúc này cho phép một người có thể yêu cầu các bên bên ngoài nắm giữ tiền và thay mặt họ tính toán các hợp đồng tương tự như một công cụ khai thác, nhưng thay vào đó, Plasma chạy trên một chuỗi khối hiện có để một người không cần tạo giao dịch trên chuỗi cơ bản cho mọi trạng thái cập nhật (bao gồm thêm các mục nhập sổ cái của người dùng mới), với dữ liệu tối thiểu trên chuỗi để cập nhật trạng thái hợp nhất.



Hình 2.4: Tạo chuỗi Plasma để mở rộng hợp đồng thông minh

Hình 2.4: Bất kỳ ai cũng có thể tạo chuỗi Plasma tùy chỉnh để có khả năng mở rộng hợp đồng thông minh cho nhiều trường hợp sử dụng khác nhau. Plasma là một loạt các hợp đồng thông minh cho phép nhiều chuỗi khối trong một chuỗi khối gốc. Chuỗi khối gốc thực thi trạng thái trong chuỗi Plasma. Chuỗi gốc là công cụ thực thi tất cả tính toán trên toàn cầu, nhưng chỉ được tính toán và bị phạt nếu có bằng chứng gian lận. Nhiều chuỗi khối Plasma có thể cùng tồn tại với logic kinh doanh và các điều khoản hợp đồng thông minh của riêng chúng. Trong Ethereum, Plasma sẽ bao gồm các hợp đồng thông minh EVM chạy trực tiếp trên Ethereum, nhưng chỉ xử lý các cam kết nhỏ có thể đại diện cho một số lượng cực lớn các mục tính toán và sổ cái tài chính trong các trường hợp không phải Byzantine.

Plasma bao gồm năm thành phần chính: (1) Một lớp khuyến khích cho các hợp đồng tính toán liên tục theo cách hiệu quả về mặt kinh tế, (2) cấu trúc để sắp xếp các chuỗi con ở định dạng cây để tối đa hóa hiệu quả chi phí thấp và thanh toán ròng các giao dịch, (3) khung tính toán MapReduce để xây dựng gian lận bằng chứng về sự chuyển đổi trạng thái trong các chuỗi lồng nhau này để tương thích với cấu trúc cây trong khi sắp xếp lại các chuyển đổi trạng thái để có khả năng mở rộng cao, (4) một cơ chế đồng thuận phụ thuộc vào chuỗi khối gốc cố gắng sao chép kết quả của các khuyến khích đồng thuận của Nakamoto và (5) cấu trúc cam kết bitmap-UTXO để đảm bảo chuyển đổi trạng thái chính xác khỏi chuỗi khối gốc đồng thời giảm thiểu chi phí thoát hàng loạt. Cho phép thoát khi không có dữ liệu hoặc hành vi Byzantine khác là một trong những điểm thiết kế chính trong hoạt động của Plasma.

#### ***a. Bằng chứng Cổ phần Plasma***

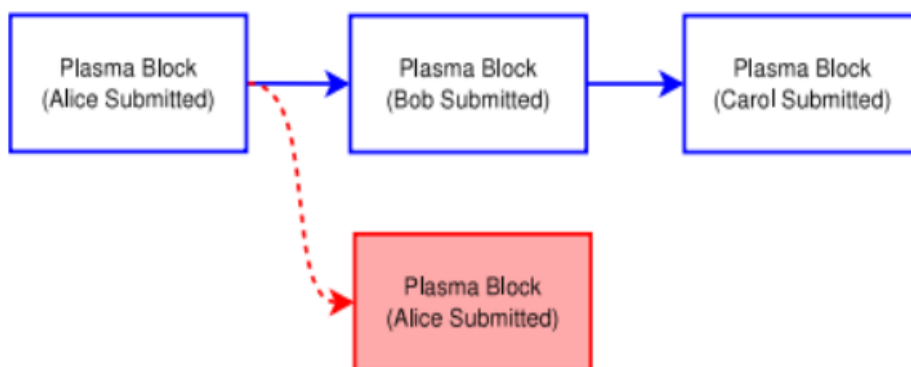
Mặc dù có thể thay mặt người khác giữ tiền bằng một trình xác thực duy nhất, những Polygon đề xuất một phương pháp như sau: một bên có thể thực thi trạng thái bằng một bộ trình xác thực, thường là trong khuôn khổ bằng chứng cổ phần yêu cầu liên kết ETH hoặc liên kết trong mã thông báo, ví dụ: ERC-20. Cơ chế đồng thuận cho hệ thống bằng chứng cổ phần này được thực thi trong một Hợp đồng thông minh trên chuỗi khối. Những nhà sáng lập cố gắng tái tạo các tiện ích xung quanh đồng thuận Nakamoto, nhưng sử dụng trái phiếu Proof of Stake. Những nhà sáng lập tin rằng một trong những cơ chế khuyến khích hữu ích hơn được xây dựng như kết quả của cơ chế Nakamoto là có động lực đáng kinh ngạc để giảm thiểu khối, trì hoãn các cuộc tấn công. Điều này là do các nhà lãnh đạo chỉ được bầu theo xác suất. Lãnh đạo là xác suất được biết đến theo thời gian (trong triển khai ban đầu, đó là 6 xác nhận).

Khi một người tìm thấy một khối, người ta khá chắc chắn rằng họ có khả năng là người dẫn đầu, nhưng họ vẫn chưa chắc chắn nếu họ là người lãnh đạo. Để đảm bảo rằng họ là người dẫn đầu, họ tuyên truyền các khối của mình cho tất cả những người tham gia trên mạng để tối đa hóa tỷ lệ cược của họ.

Các liên minh bằng chứng cổ phần phải đối mặt với vấn đề này vì có thể xảy ra nếu một người trực tiếp bầu chọn người đứng đầu, ngăn chặn các cuộc tấn công giữ lại của các tập đoàn đa số (cũng được khái quát hóa là "sự sẵn có của dữ liệu vấn đề") trở nên phóng đại.

Những nhà sáng lập có thể giảm thiểu điều này trong bằng chứng cổ phần Plasma (Plasma PoS) bằng cách cho phép các bên liên quan xuất bản trên chuỗi khối gốc hoặc chuỗi Plasma mẹ chứa hàm băm đã cam kết của chuỗi khối mới của chúng. Trình xác thực chỉ xây dựng dựa trên các khối mà chúng đã xác thực đầy đủ. Họ có thể xây dựng trên các khối song song (để khuyến khích chia sẻ thông tin tối đa). Họ tạo ra các ưu đãi để người xác thực đại diện cho 100 khối trước đây để khớp với tỷ lệ người đặt cược hiện tại (tức là nếu một người đặt cược 3 phần trăm số tiền, chúng phải là 3 phần trăm trong số 100 khối trước đây), bởi vì thường nhiều phí giao dịch hơn để được thanh toán cho đại diện chính xác. lệ phí

quá mức (do hành vi dưới mức tối ưu của những người đặt cược) chuyển đến một nhóm để trả phí trong tương lai. Một cam kết tồn tại trong mọi khối bao gồm dữ liệu từ 100 khối trước đây (với nonce). Chuỗi chính xác là chuỗi có tổng trọng lượng của các khoản phí cao nhất. Sau một khoảng thời gian, các khối được hoàn thành.



*Hình 2.5: Trình xác thực gửi yêu cầu qua khối Plasma*

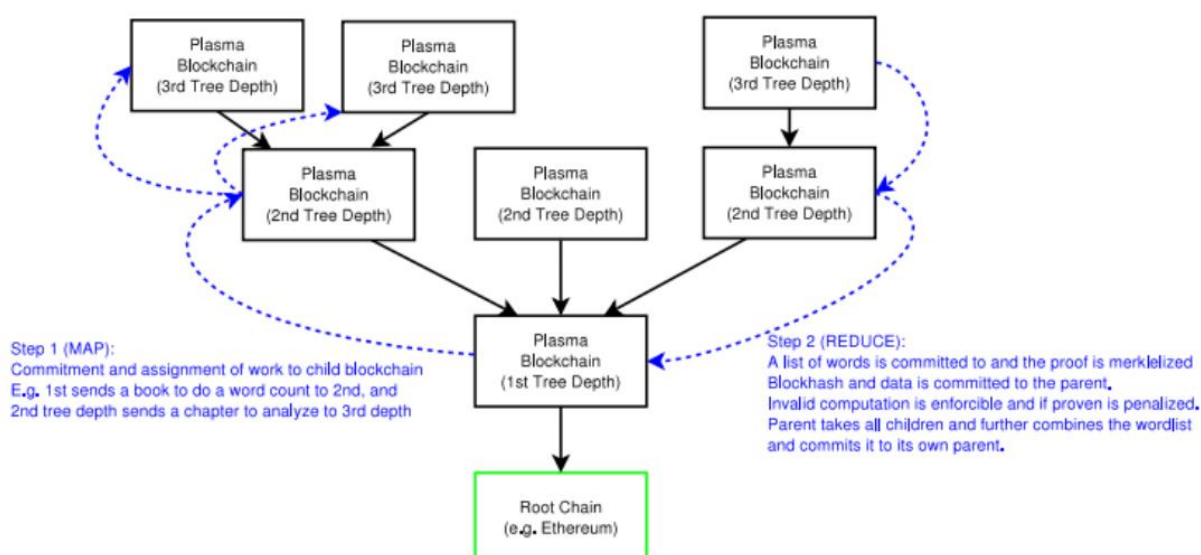
Hình 2.5: Giả sử rằng Alice, Bob và Carol là 3 trình xác thực có trọng số bằng nhau. Họ được khuyến khích xây dựng cấu trúc vòng tròn để thu được lợi nhuận tối đa. Những cam kết này là được gửi tới chuỗi gốc. Đầu chuỗi phụ thuộc vào điểm trọng lượng tối đa bằng cách phân phối chính xác của các khối trong n khoảng thời gian (màu xanh nước biển là đầu chuỗi ứng cử viên hiện tại, màu đỏ là một phần tử đơn độc). Chuỗi dưới mức tối ưu có bất kỳ khoản phí vượt quá nào được đưa vào nhóm dành cho những người xác thực trong tương lai với độ chính xác cao hơn một số ngưỡng (ví dụ: 90%). Sau khoảng thời gian n, người ta cho rằng đầu chuỗi màu xanh nước biển đã hoàn thành.

Điều này khuyến khích người tham gia tham gia và nhân rộng các giả định tấn công 51% trong sự đồng thuận của Nakamoto. Trong trường hợp một chuỗi bị tấn công thông qua giữ lại khối hoặc cách khác hành vi Byzantine, những người tham gia không phải Byzantine tiến hành rút tiền hàng loạt trên chuỗi khối gốc. Nếu liên kết cho chuỗi Plasma gốc cao nhất ở dạng của mã thông báo, có khả năng giá trị của mã thông báo sẽ giảm giá trị đáng kể do khối lượng lỗi ra.

### ***b. Chuỗi khối dưới dạng MapReduce***

Bằng cách xây dựng tính toán theo định dạng MapReduce, cũng dễ dàng thiết kế tính toán và chuyển đổi trạng thái trong một cây phân cấp.

MapReduce đưa ra một khuôn khổ để tính toán quy mô lớn trên hàng nghìn nút. Chuỗi khối phải đối mặt với các vấn đề tương tự trong việc đáp ứng quy mô tính toán, nhưng có các yêu cầu bổ sung trong việc tạo bằng chứng tính toán.



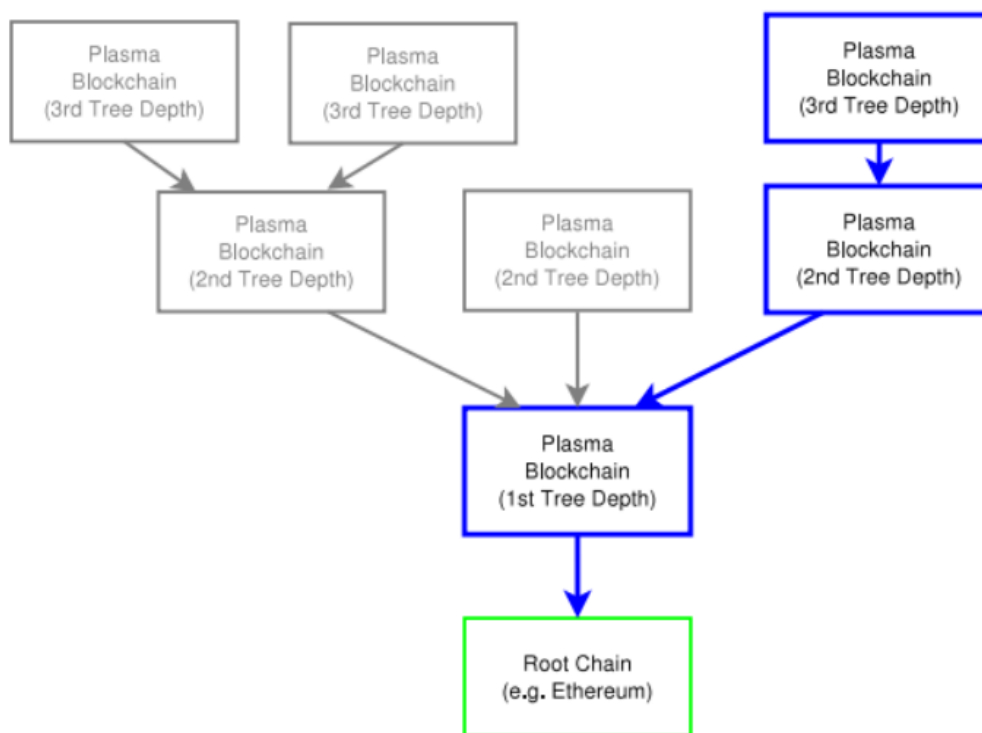
Hình 2.6: Mô hình chuỗi khối dưới dạng MapReduce

Hình 2.6: Màu xanh nước biển là các thông điệp được truyền trong khối cha cho các khối con. Các nút con phải cam kết khối chính trong một số n khối nếu không sẽ phải đối mặt với việc tạm dừng chuỗi. Dữ liệu khối phân phối công việc cho những đứa trẻ đang cam kết tính toán. Nút cấp 3 thực hiện tính toán và trả về một danh sách từ (ví dụ: 3 lần xuất hiện của từ "Xin chào", 2 lần xuất hiện của từ "Thế giới" trong chương chúng chịu trách nhiệm tính toán). Dữ liệu danh sách từ được trả lại cho cha mẹ như một phần của cam kết, danh sách từ được kết hợp với nhau từ trẻ em và gửi cho phụ huynh, cuối cùng hoàn thành một danh sách từ toàn cầu (ví dụ: toàn bộ kho văn bản chứa 100 trường hợp của "Xin chào" và 150 trường hợp của từ "Thế giới"). Điều này tạo ra khả năng tính toán hiệu quả về mặt kinh tế ở quy mô lớn, chỉ với một tiêu đề khối, hàm băm cam kết trên chuỗi gốc để bao gồm lượng dữ liệu và công việc rất cao. Chỉ khi một khối bị lỗi bằng chứng về tính không hợp lệ đó được xuất bản, nếu không thì lượng dữ liệu cực kỳ tối thiểu được gửi trên thư mục gốc chuỗi theo định kỳ.

Những nhà sáng lập đề xuất một phương pháp theo đó giai đoạn bản đồ bao gồm các cam kết về dữ liệu để tính toán làm đầu vào và trong bước rút gọn bao gồm bằng chứng chuyển đổi trạng thái được merkleized khi trả về kết quả. Quá trình chuyển đổi trạng thái merkleized được thực thi thông qua bằng chứng gian lận được xây dựng trên chuỗi khối gốc. Cũng có thể xây dựng bằng chứng zk-SNARKs của các chuyển trạng thái. Đối với một số cấu trúc tính toán, một bitmap về chuyển đổi trạng thái cũng có thể cần thiết trong bước rút gọn (do đó có thể sử dụng nhiều hơn một bit cho mỗi tài khoản cho các trường hợp sử dụng này).

Cấu trúc của chúng tôi cho phép tính toán quy mô lớn đáng kinh ngạc, với sự đánh đổi về thời gian hoặc tốc độ. Những sự đánh đổi này tạo ra một mạng nơi các nút khẳng định tính toán và những người tham gia chịu trách nhiệm xác minh chúng. Điều này không tạo ra một hệ thống theo đó người ta có thể thuê ngoài hoàn toàn tính toán mà không cần tin tưởng, nó cho phép khả năng nén tính toán thành bằng chứng ngoại quan. Những bằng chứng ngoại quan này khuyến khích người tham gia chỉ chứng thực những điều Thành thật. Điều này một lần nữa, theo tường thuật trong Lightning Network, theo đó nếu một cái cây đổ trong rừng và không ai lắng nghe nó, nó cho rằng việc nó có tạo ra hay không cũng không quan trọng. một âm thanh hay không. Tương tự, nếu không có ai theo dõi/thực thi tính toán, thì nó được cho là là đúng, hoặc đơn giản là kết quả có thể ra sao không quan trọng. Tính toán có thể được theo dõi bởi bất kỳ người tham gia nào trong các mạng mở, nhưng những người tham gia giữ sổ dư và/hoặc yêu cầu tính toán chính xác sẽ theo dõi chuỗi định kỳ để đảm bảo tính chính xác. Các lợi ích mở rộng đến từ việc loại bỏ yêu cầu giám sát các chuỗi mà người ta không bị ảnh hưởng về mặt kinh tế, người ta nên theo dõi các chuỗi mà người ta muốn thực thi đúng hành vi. Hành vi trên các chuỗi Plasma khác có thể được kết hợp với nhau như một phần của bước giảm để tính toán ảnh hưởng đến một được thể hiện ở trạng thái tối thiểu. Ví dụ, đối với một sàn giao dịch phi tập trung, người ta không quan tâm đến việc các đối tác nào sắp xếp theo thứ tự nào, họ chỉ cần xem một sổ lệnh hợp nhất, vì vậy một người chỉ cần quan sát tất cả các chuỗi khác với tư cách là một đối tác duy nhất, trong khi chuỗi của chính một người được xác thực đầy đủ để thực thi các giao dịch và thứ tự điền vào đúng người (bao gồm cả chính mình). Một ví dụ khác là người ta có thể xây dựng BBS

trên cây chuỗi Plasma và người ta không cần nhận các bản cập nhật trên chủ đề mà người ta không quan tâm.



Hình 2. 7: Xây dựng BBS trên cây chuỗi Plasma

Hình 2.7: Người ta chỉ cần xem dữ liệu mà người ta muốn thực thi. Nếu hoạt động kinh tế hoặc tính toán xảy ra trên các chuỗi Plasma khác không cần thiết phải thực thi (màu xám), người ta có thể coi tất cả các chuỗi khác là một đối tác duy nhất. Ví dụ, trong một trao đổi phi tập trung Plasma, người ta chỉ cần xem các chuỗi mà ảnh hưởng đến cam kết của một người (màu xanh đậm).

#### 2.1.5. Vấn đề an toàn của Polygon

Mô hình bảo mật của Polygon cung cấp ba loại mô hình bảo mật để những nhà phát triển xây dựng Dapp dựa trên:

- Bảo mật bằng chứng cổ phần (Proof of Stake security)
- Bảo mật Plasma
- Bảo mật kết hợp Plasma + PoS

##### Bảo mật PoS

Bảo mật Proof of Stake (PoS) được cung cấp bởi lớp Heimdall & Bor được xây dựng trên Tendermint. Một điểm kiểm tra chỉ được cam kết với chuỗi gốc khi  $\frac{2}{3}$  số người xác thực đã ký vào đó. Để kích hoạt cơ chế PoS trên nền tảng Polygon, có sử dụng một bộ hợp đồng quản lý đặt cược trên Ethereum, cũng như một bộ trình xác thực được khuyến khích chạy các nút Heimdall và Bor. Điều này thực hiện các tính năng sau:

- Khả năng cho bất kỳ ai đặt cược mã thông báo MATIC trên hợp đồng thông minh Ethereum và tham gia hệ thống với tư cách là Validator (người xác thực)

- Kiểm phần thưởng đặt cược khi xác thực chuyển đổi trạng thái trên Polygon

Cơ chế PoS cũng hoạt động như một biện pháp giảm thiểu vấn đề không có sẵn dữ liệu cho các sidechain về mặt Plasma.

Polygon có một lớp kết thúc nhanh giúp hoàn thiện trạng thái sidechain theo định kỳ thông qua các điểm kiểm tra. Sự kết thúc nhanh chóng giúp Polygon củng cố trạng thái sidechain. Chuỗi tương thích với EVM có ít trình xác thực và thời gian tạo khối nhanh hơn với thông lượng cao. Nó chọn khả năng mở rộng trên mức độ phân cấp cao. Heimdall đảm bảo rằng cam kết trạng thái cuối cùng là bảo vệ và chuyển qua một bộ trình xác thực lớn và do đó có tính phân cấp cao.

#### Bảo mật *Plasma*

Polygon cung cấp "Plasma Guarantees" đối với các tình huống tấn công khác nhau. Hai trường hợp chính được xem xét là:

- Toán tử chuỗi (trong Polygon, lớp Heimdall) bị hỏng
- Người dùng bị hỏng

Trong cả hai trường hợp, nếu tài sản của người dùng trên chuỗi plasma bị xâm phạm, họ cần bắt đầu thoát hàng loạt. Polygon cung cấp các cấu trúc trên hợp đồng thông minh rootchain có thể được tận dụng.

Thực tế, bảo mật được cung cấp bởi các hợp đồng Plasma của Polygon cũng trên bảo mật của Ethereum. Tiền của người dùng chỉ gặp rủi ro nếu Ethereum thất bại. Nói một cách đơn giản, chuỗi plasma an toàn như cơ chế đồng thuận của chuỗi chính. Điều này có thể ngoại suy để nói rằng chuỗi plasma có thể sử dụng các cơ chế đồng thuận thực sự đơn giản mà vẫn an toàn.

Ngoài bảo mật Plasma và bảo mật Proof of Stake có thể có trong các Dapp được triển khai trên Polygon, còn có một cách tiếp cận kết hợp mà các nhà phát triển có thể làm theo - điều này đơn giản có nghĩa là đảm bảo cả Plasma và Proof of Stake trên một số quy trình công việc cụ thể của Dapp.

#### **2.1.6. Ưu điểm và nhược điểm Polygon**

##### *Ưu điểm*

- Polygon được biết đến với thế mạnh về việc tối ưu hóa khả năng mở rộng nền tảng và độ tức thì của các giao dịch blockchain. Trong đó, khung plasma tùy chỉnh là một trong những công nghệ được đánh giá là độc đáo nhất trên hệ Polygon, được xây dựng trên các checkpoint bằng chứng cổ phần, chạy qua chuỗi Ethereum. Nhờ vậy, mỗi sidechain có thể đạt đến con số tối đa là 65.536 giao dịch trên mỗi khối thuộc Polygon.

- Bên cạnh đó, Polygon còn sở hữu những thiết kế nhằm hỗ trợ sự phát triển của DeFi (giao thức tài chính phi tập trung), dựa vào những sidechain có sẵn trong hệ sinh thái của Ethereum. Một số điểm hạn chế còn tồn tại trong những dự án tập trung vào khả năng tương tác như Cosmos hay Polkadot cũng đã được giao thức của Polygon xây dựng và giải quyết. Người dùng có thể dễ dàng lập trình trong Solidity và xây dựng ứng dụng trên Ethereum, nhờ khả năng tương thích với máy ảo EVM của Polygon. Cuối cùng, Polygon còn có thể đem đến cho bạn mô hình bảo mật hoàn toàn tùy chọn. Bởi vậy, việc hy sinh tính linh hoạt hay độc lập để đảm bảo an ninh bổ sung đối với các nền tảng chủ quyền sẽ không bao giờ xảy ra. Polygon đủ sự linh hoạt và luôn trong trạng thái sẵn sàng để kết hợp các giải pháp khả năng mở rộng khả quan.



### *Hạn chế*

– Điểm hạn chế duy nhất của nền tảng này nằm ở việc nó được thiết kế và xây dựng chỉ để hỗ trợ cho Ethereum basechain.

#### 1.2.1. Giới thiệu về cách tạo ra 1 đồng token

#### 1.2.2. Cách thiết kế mantic token

#### 1.2.3. Giới thiệu đồng token Mantic

#### 1.2.5. Vấn đề bảo mật

### 1.3. Kết luận chương

## CHƯƠNG 3: Triển Khai thực tế

### 1. Cài đặt

#### 1.1. Cài đặt Node JS

Node.js là một hệ thống phần mềm được thiết kế để viết các ứng dụng internet có khả năng mở rộng, đặc biệt là máy chủ web. Chương trình được viết bằng JavaScript, sử dụng kỹ thuật điều khiển theo sự kiện, nhập/xuất không đồng bộ để tối thiểu tổng chi phí và tối đa khả năng mở rộng.

Link tải bộ cài đặt Node JS: <https://nodejs.org/en/download>



Hình 1.1: Node.js

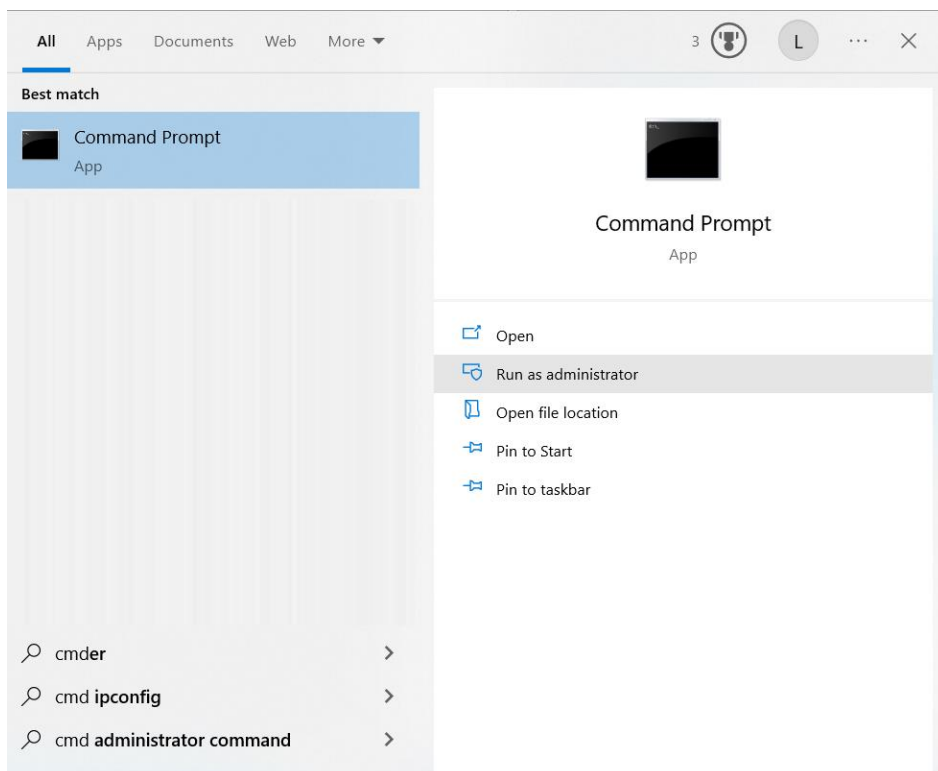
## 1.2.Cài đặt tiện ích Yarn cho Node JS

Yarn là một tiện ích giúp quản lý package cho Node.js. Nó tập trung vào tốc độ, bảo mật và tính nhất quán. Yarn đặc biệt phổ biến và khá được ưa thích trong thế giới lập trình React.



Hình 1.2.1: Yarn

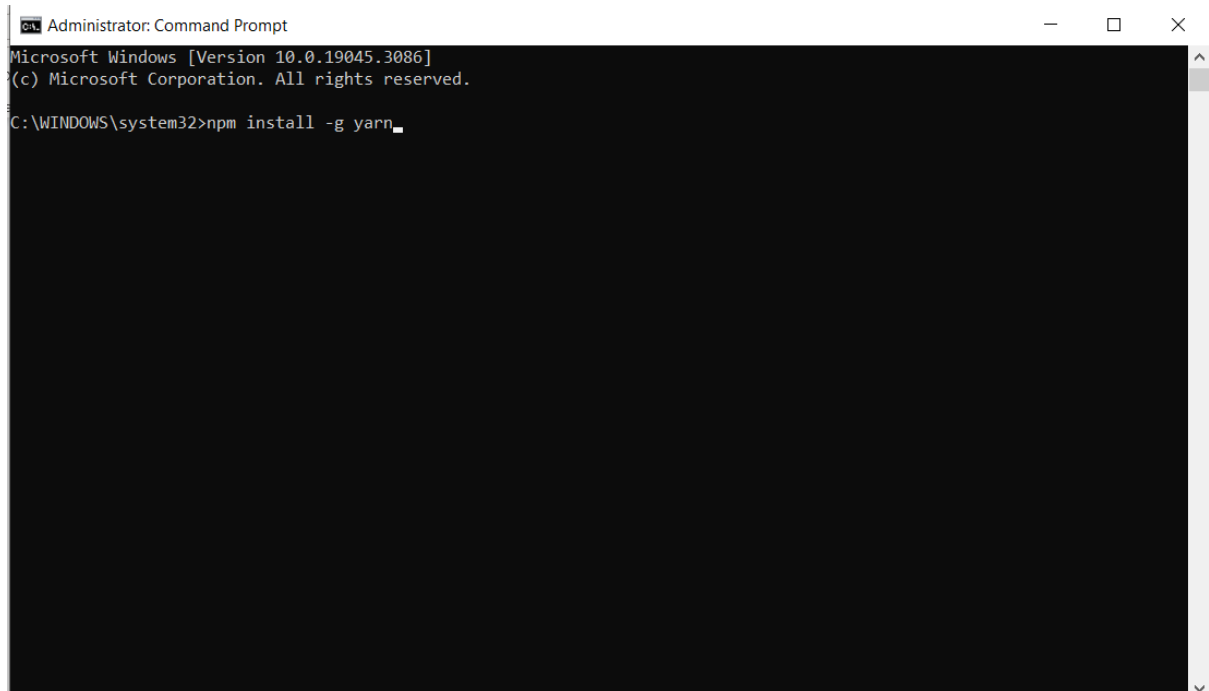
Để cài đặt yarn, trước tiên ta chạy command prompt dưới quyền administrator



Hính 1.2.2: Mở Command Prompt dưới quyền Administrator

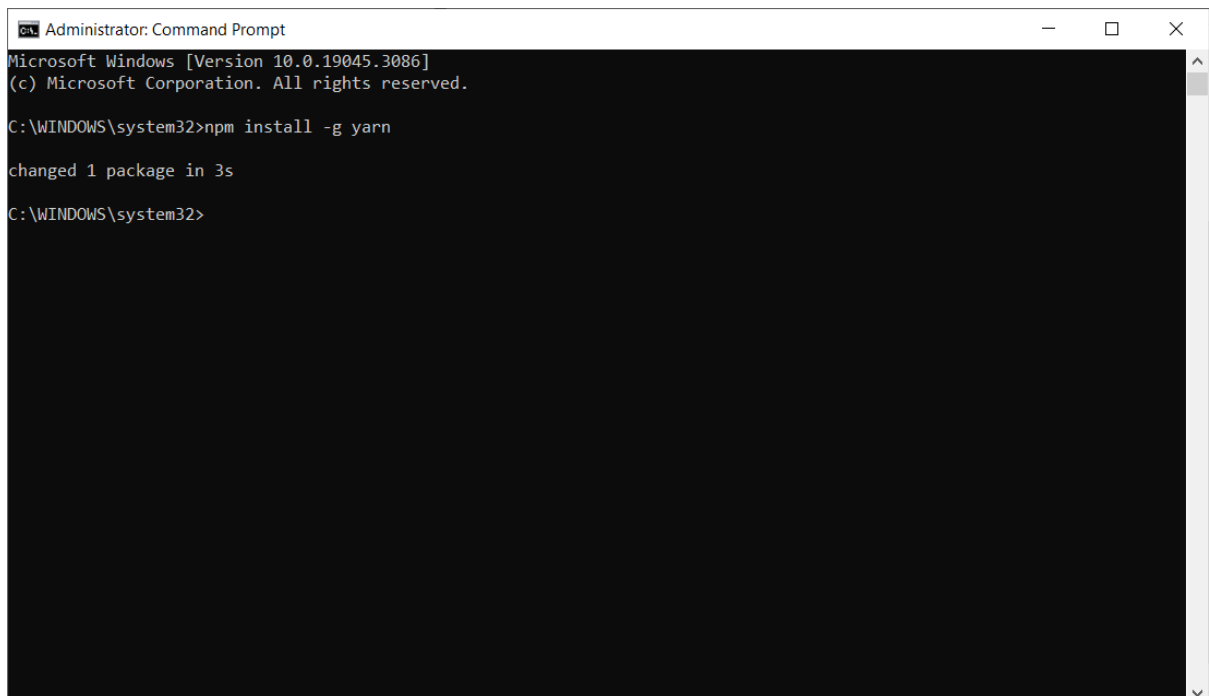
Tiếp theo, trên màn hình command prompt, ta nhập lệnh:

`npm install -g yarn`



Hình 1.2.3: Chạy lệnh cài đặt Yarn trong Command Prompt

Sau khi nhập lệnh, ta chỉ việc chờ cài đặt. Sau khi cài đặt xong, sẽ trông như thế này:



Hình 1.2.4: Thông báo cài đặt Yarn thành công

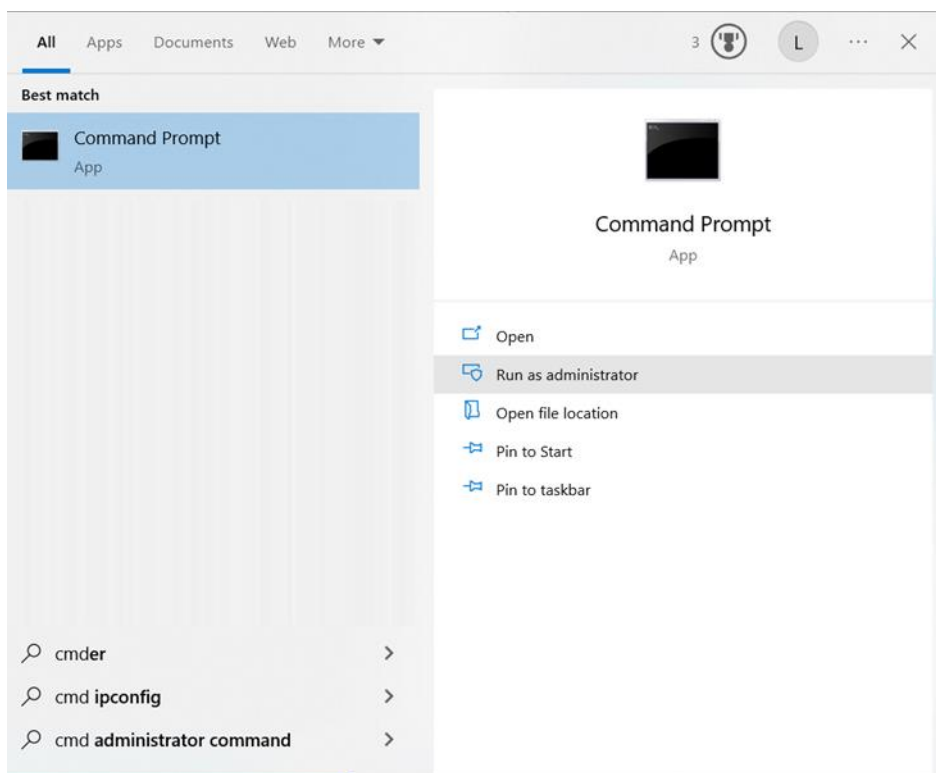
### 1.3.Cài đặt Next.js sử dụng Yarn

Next.js là một framework hỗ trợ xây dựng ứng dụng web. Với Next.js, người phát triển ứng dụng web có thể xây dựng giao diện người dùng sử dụng những components của React. Và Next.js cũng cung cấp thêm cho lập trình viên phát triển ứng dụng web một số cấu trúc, tính năng và tối ưu hóa nhất cho ứng dụng web của lập trình viên.



Hình 1.3.1: Next.js

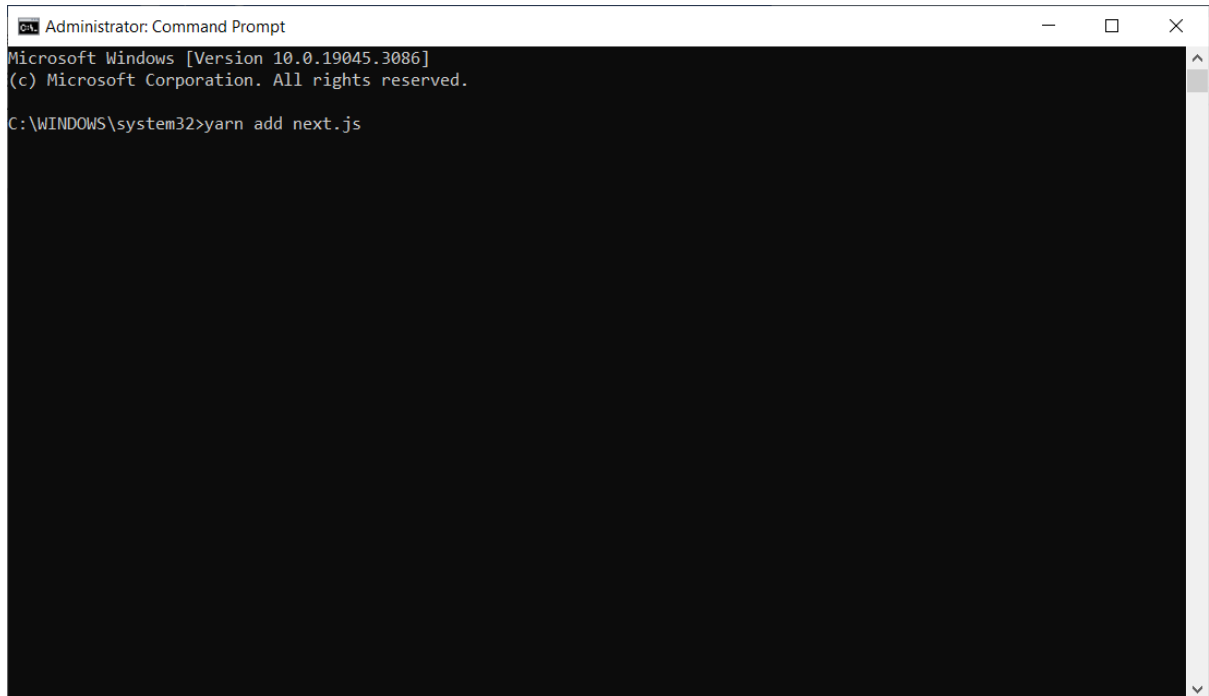
Để cài đặt Next.js, ta mở command prompt dưới quyền administrator:



Hình 1.3.2: Mở Command Prompt dưới quyền Administrator

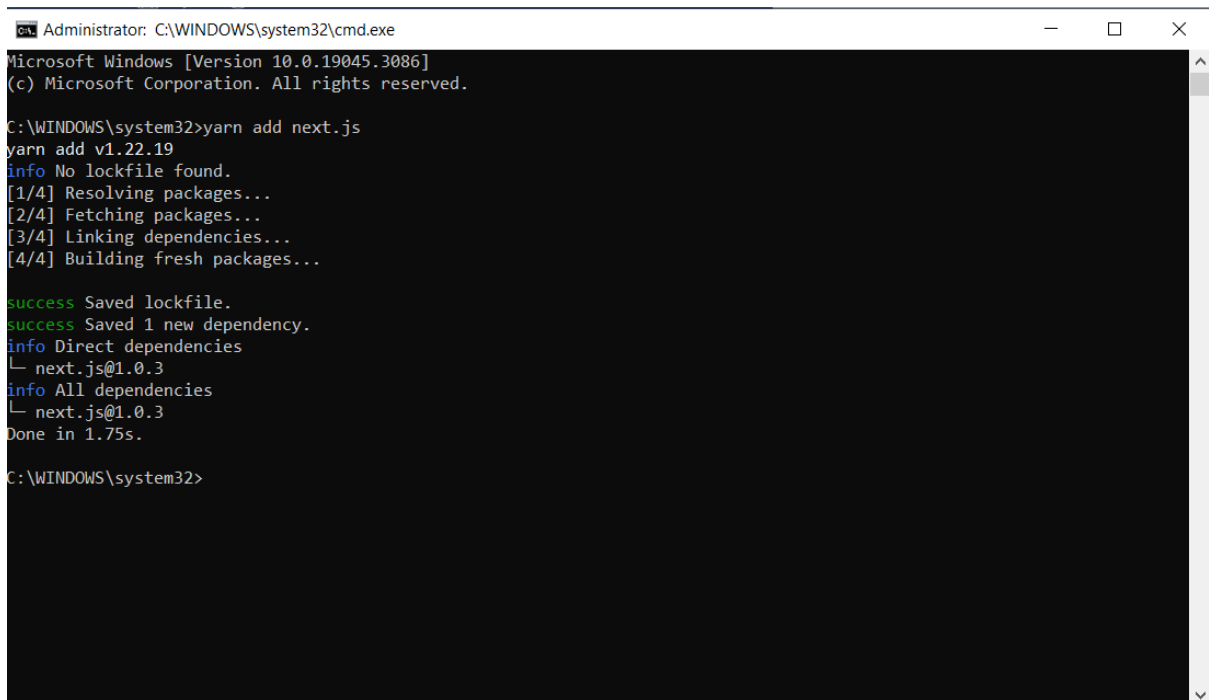
Tiếp theo, trong giao diện command prompt, ta nhập lệnh:

yarn add next.js



Hình 1.3.3: Chạy lệnh cài đặt Next.js thông qua Yarn

Sau khi cài xong next.js, ta sẽ nhận được thông báo như thế này trên màn hình command prompt:



Hình 1.3.4: Thông báo xuất ra sau khi cài đặt Next.js thành công

#### 1.4.Cài đặt trang web NFT Cards

Trang web NFT Cards là trang web được phát triển bởi nhóm chúng em dựa trên một mã nguồn mở được cung cấp bởi Thirdweb và kết hợp với các tiện ích mà Thirdweb hỗ trợ (như: Deploy nhanh NFT, NFT Packs, Marketplace Smart Contracts).

Trang web này là trung tâm, nơi chúng em và cả người chơi (khách hàng) của game chúng em trong tương lai sẽ giao dịch, trao đổi NFT Cards với nhau.



Hình 1.4.1: Ứng dụng web NFT Cards.

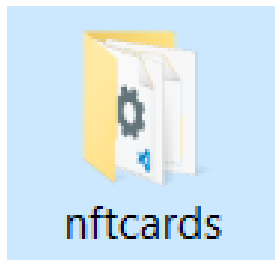
Để có thể cài đặt trang web NFT Cards, trước tiên ta cần tải source code trang web hay clone repository của trang web về thông qua link:

<https://www.github.com/lequochai26/nftcards>

lequochai26 Update README.md		c5e5e7d 2 days ago	7 commits
components	Update 15/06/2023	4 days ago	
const	Update 15/06/2023	4 days ago	
pages	Update 15/06/2023	4 days ago	
public	Initial commit	last week	
scripts	Update 15/06/2023	4 days ago	
styles	Update 15/06/2023	4 days ago	
.env	Initial commit	last week	
.eslintrc.json	Initial commit	last week	
.gitattributes	Initial commit	last week	
.gitignore	Initial commit	last week	
LICENSE.md	Initial commit	last week	
README.md	Update README.md	2 days ago	
next-env.d.ts	Initial commit	last week	
next.config.js	Initial commit	last week	
package.json	Initial commit	last week	
tsconfig.json	Initial commit	last week	
yarn.lock	Initial commit	last week	

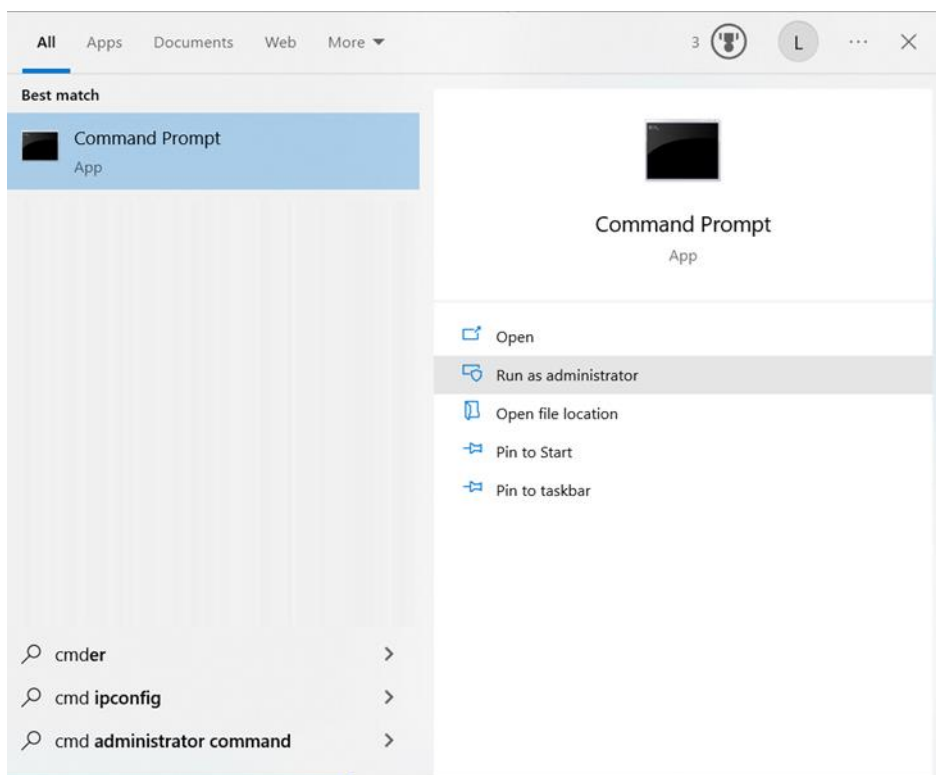
Hình 1.4.2: Mã nguồn ứng dụng web NFT Cards

Sau khi tải source code về, nếu source code đang được nén trong file .zip, ta sẽ tiến hành giải nén file và thu về thư mục source code như hình:



Hình 1.4.3: Thư mục mã nguồn ứng dụng web NFT Cards

Bây giờ, chúng ta sẽ cần phải mở command prompt dưới quyền administrator để tiến hành khởi chạy trang web:



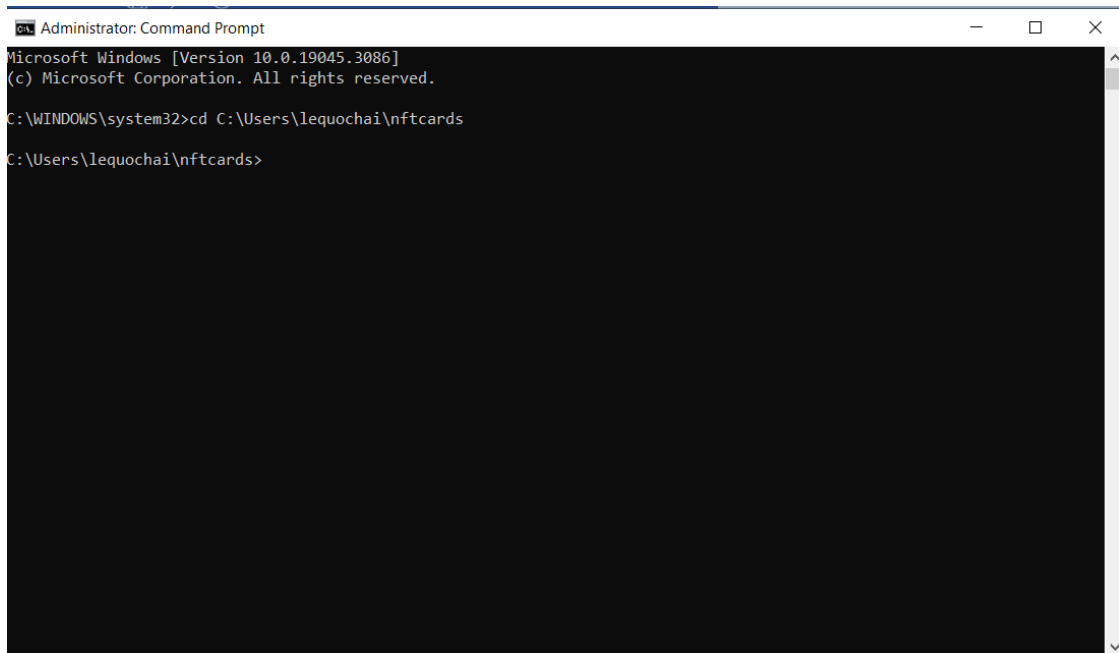
Hình 1.4.4: Mở Command Prompt dưới quyền Administrator



Hiện tại, ở giao diện Command Prompt, lúc này Command Prompt đang trở đến thư mục khác và để Cmd trở về đúng thư mục nftcards mình đang cần dùng, ta chạy lệnh:

cd (đường dẫn đến thư mục nftcards ta đã giải nén ở trên)

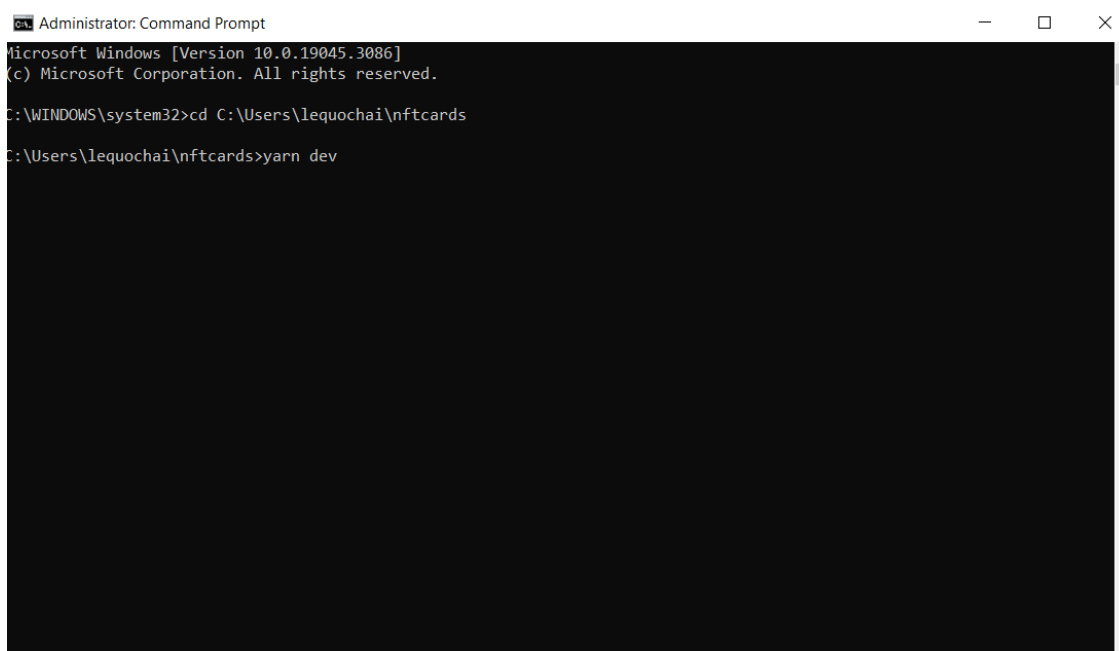
trong trường hợp này là: cd C:\Users\lequochai\nftcards



Hình 1.4.5: Thay đổi vị trí Command Prompt trở tới

Sau khi chúng ta đã trở Command Prompt về đúng thư mục cần dùng, ta chạy lệnh:

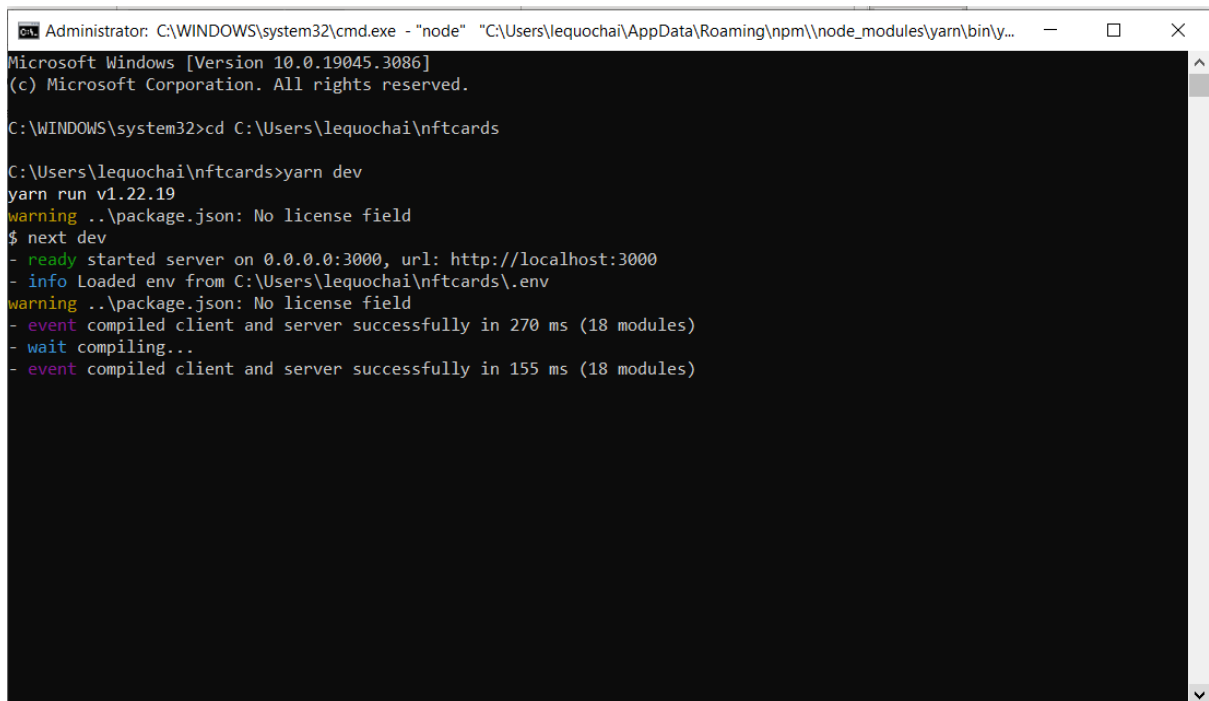
yarn dev



Hình 1.4.6: Chạy ứng dụng web NFT Cards



Lúc này, sẽ mất vài giây hoặc có thể đến vài phút để biên dịch và khởi chạy trang web chúng ta. Và sau khi đã thành công biên dịch và khởi chạy, ta sẽ nhận được thông báo từ Command Prompt như sau:



```
Administrator: C:\WINDOWS\system32\cmd.exe - "node" "C:\Users\lequochai\AppData\Roaming\npm\node_modules\yarn\bin\yarn..."
Microsoft Windows [Version 10.0.19045.3086]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\lequochai\nftcards

C:\Users\lequochai\nftcards>yarn dev
yarn run v1.22.19
warning ..\package.json: No license field
$ next dev
- ready started server on 0.0.0.0:3000, url: http://localhost:3000
- info Loaded env from C:\Users\lequochai\nftcards\.env
warning ..\package.json: No license field
- event compiled client and server successfully in 270 ms (18 modules)
- wait compiling...
- event compiled client and server successfully in 155 ms (18 modules)
```

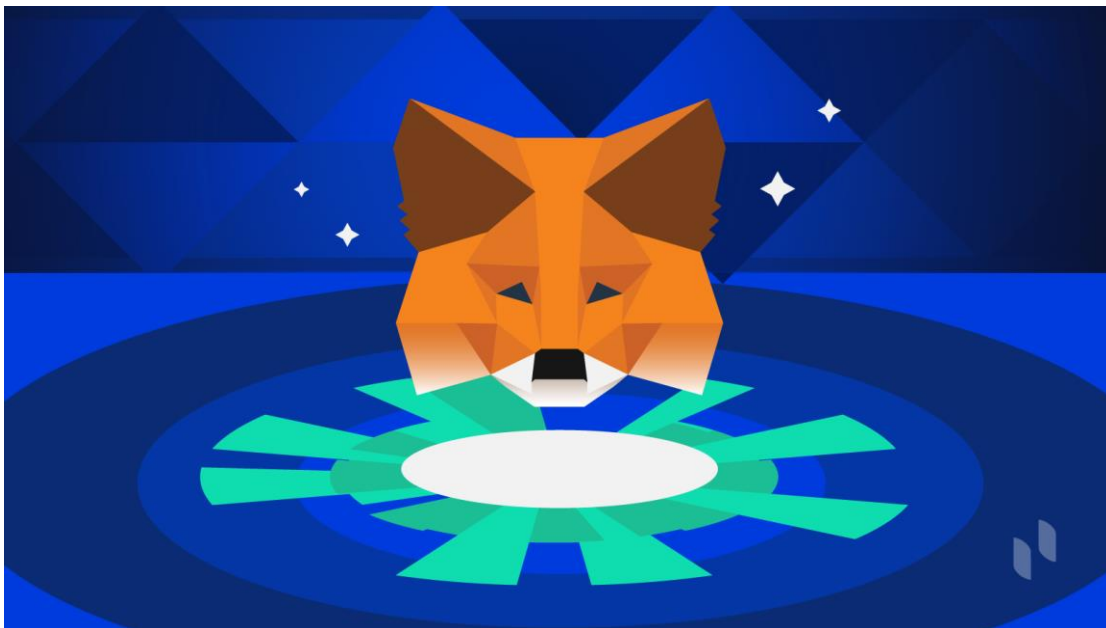
Hình 1.4.7: Chạy ứng dụng thành công

### 1.5.Cài đặt ví tiền mã hóa (Bỏ qua nếu đã cài đặt hoặc đang sử dụng một ví khác)

Vì trang web NFT Cards do nhóm em phát triển sẽ thực hiện giao dịch, trao đổi, mua bán với nhau bằng cryptocurrency (Tiền mã hóa). Vì vậy, để có thể sử dụng chương trình, ta cần phải cài ví tiền mã hóa.

Trong trường hợp này, em đề xuất sử dụng ví tiền mã hóa MetaMask. Vì MetaMask vừa dễ cài đặt vừa dễ sử dụng lại tốn rất ít thời gian để khởi tạo ví mới, tài khoản mới.

MetaMask là một chương trình ví tiền mã hóa được sử dụng để tương tác với mạng Blockchain của Ethereum. Nó cho phép người dùng truy cập vào ví Ethereum của họ thông qua một tiện ích được tích hợp cùng với trình duyệt web hoặc một ứng dụng mobile và nó còn được dùng để tương tác với các ứng dụng phi tập trung (decentralized applications).



Hình 1.5: Ví tiền điện tử/tiền mã hóa MetaMask

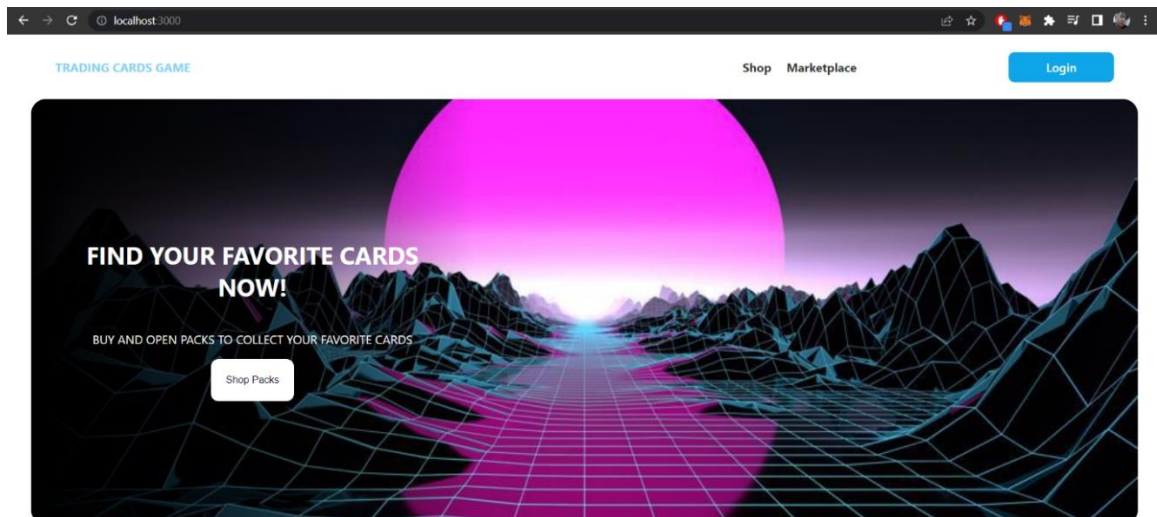
### 2.Cách vận hành và chức năng web NFT Cards

Như em đã giới thiệu ở trên, trang web NFT Cards thực tế là một thị trường cục bộ phục vụ, hỗ trợ một số chức năng như: Mở gói nhận ngẫu nhiên thẻ bài NFT, trao đổi thẻ bài NFT,... sử dụng tiền mã hóa cho trò chơi thẻ bài của nhóm chúng em đang phát triển. Và đây cũng là thị trường chính, nơi người chơi có thể kiếm thêm cho mình một khoản thu nhập nhỏ thông qua việc chơi game và trao đổi thẻ bài với nhau.

## 2.1. Truy cập trang web

Sau khi hoàn thành các bước cài đặt ở trên, ta tiến hành thử truy cập vào và chiêm ngưỡng thành quả của chúng ta.

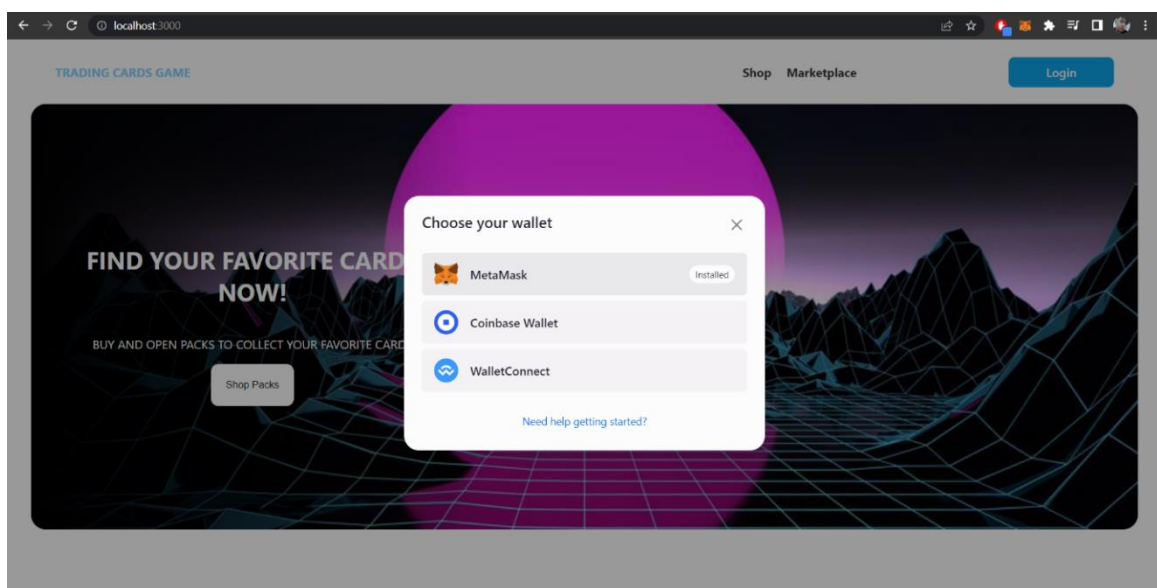
Sau khi cài đặt như hướng dẫn trên, trang web của chúng ta sẽ thuộc đường dẫn như sau: localhost:3000



Hình 2.1: Trang chủ của ứng dụng web NFT Cards

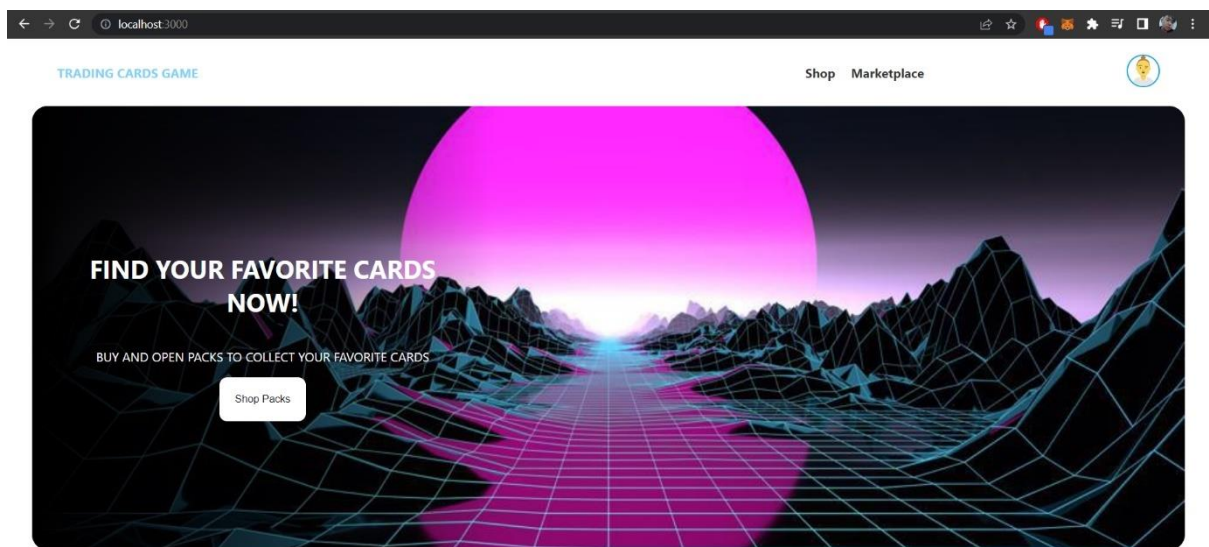
## 2.2. Đăng nhập thông qua ví tiền ảo

Trước khi thực hiện bất cứ giao dịch nào cũng như mua, bán gì thì ta cần phải đăng nhập/kết nối với ví tiền ảo của chúng ta trước. Trong trường hợp này, em sử dụng MetaMask. Vậy, để đăng nhập, ta nhấn vào nút “Login” góc phải trên màn hình.



Hình 2.2.1: Đăng nhập vào ứng dụng web NFT Cards bằng ví MetaMask

Sau khi đăng nhập, giao diện web của chúng ta sẽ như thế này:



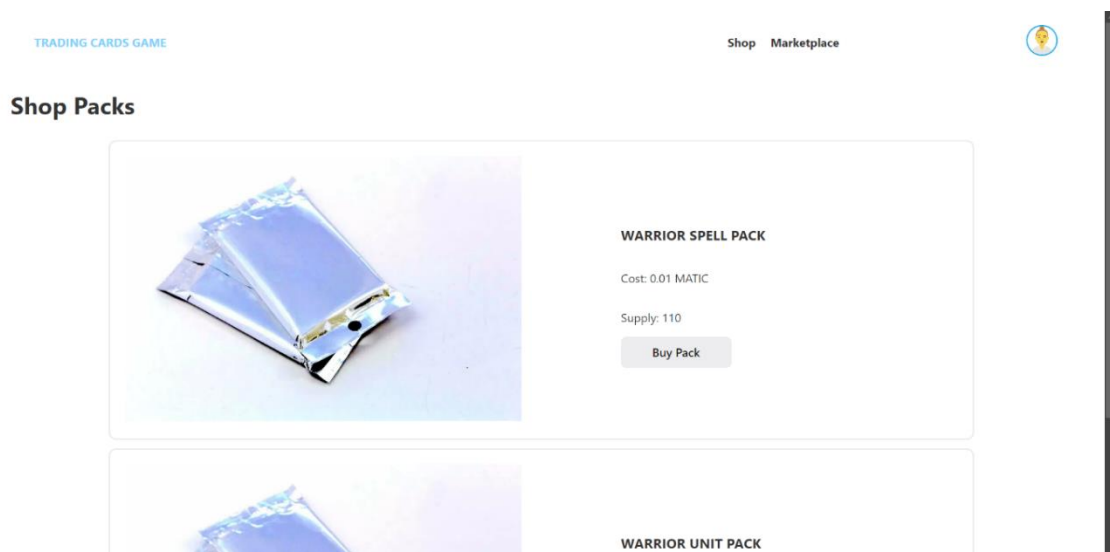
Hình 2.2.2: Giao diện củ ứng dụng sau khi đăng nhập

## 2.3. Mua và mở gói thẻ bài NFT

### 2.3.1. Truy cập vào Shop Packs

Shop Packs là nơi mà chúng em (nhóm phát triển game) đưa ra những packs thẻ bài NFT. Người chơi có thể truy cập vào và mua những packs thẻ bài này với một mức giá nhất định.

Một packs thẻ bài như vậy sẽ mở ra 5 thẻ bài ngẫu nhiên, trong đó những thẻ bài được mở ra có thể sẽ trùng nhau hoặc không cũng như là sẽ có cơ hội trúng những thẻ bài hiếm và rất hiếm (những thẻ bài chỉ có số lượng rất ít ỏi).

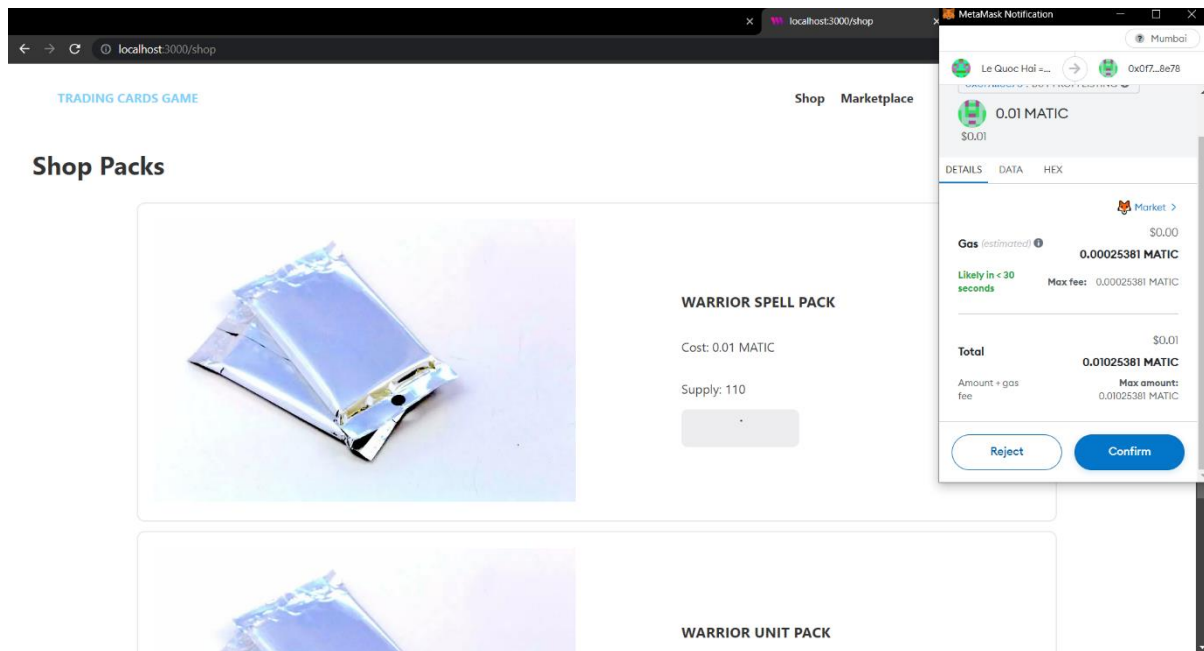


Hình 2.3.1: Trang Shop Packs của ứng dụng

### 2.3.2. Mua packs thẻ bài NFT

Để tiến hành mua 1 trong những packs thẻ bài này, ta nhấn vào nút “Buy Pack” màu trắng – xám ở packs thẻ bài NFT mà ta muốn mua.

Sẽ mất một khoảng thời gian và sẽ có một cửa sổ Popup (tùy theo ví mà ta sử dụng sẽ có cửa sổ khác nhau) yêu cầu chúng ta xác nhận giao dịch để mua packs thẻ bài này. Ta nhấn vào “Confirm” (Tùy vào mỗi ví có thể sẽ khác nhau) để xác nhận giao dịch mua packs thẻ bài này.



Hình 2.3.2: Mua pack Warrior Spell Pack và xác nhận giao dịch

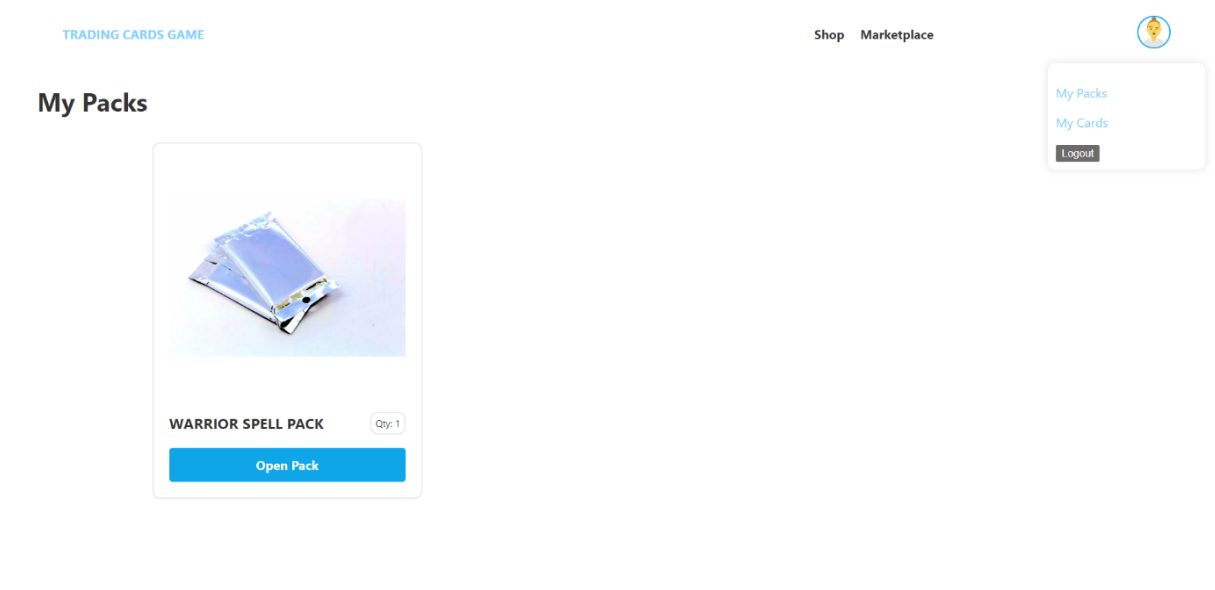
### 2.3.3. Mở packs thẻ bài NFT đã mua

#### 2.3.3.1. Truy cập vào my packs

Để truy cập vào my packs, người dùng click vào nút avatar người dùng tròn nhỏ phía góc trên bên phải giao diện.

Sau đó sẽ có một cửa sổ nhỏ hiện lên kèm theo đó là vài dòng chữ vào trong đó có dòng chữ “My Packs”. Click vào đó.

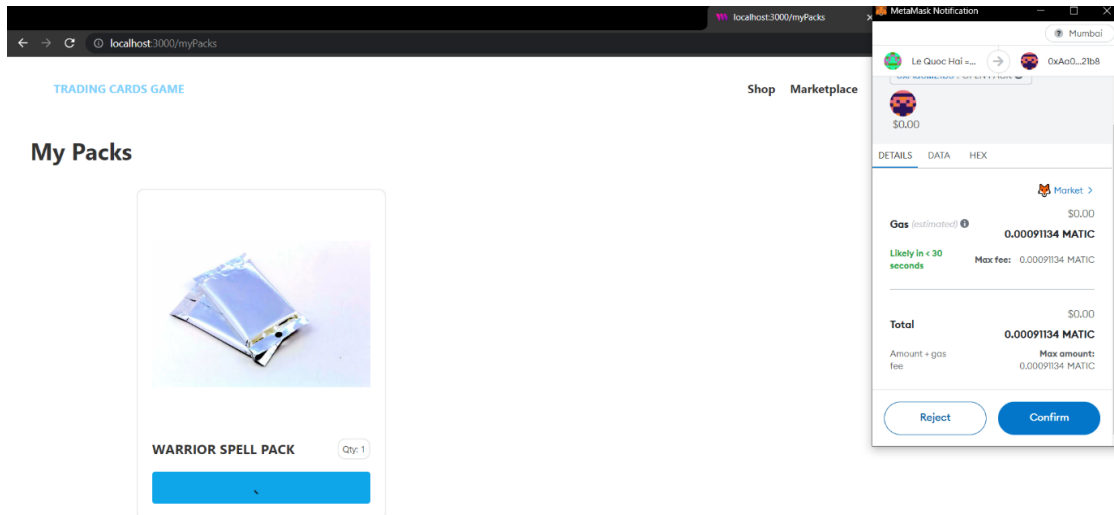
Và ta sẽ được dẫn đến trang như hình cùng với đó là sự xuất hiện của pack thẻ bài mà chúng ta đã mua ở Shop Packs.



Hình 2.3.3.1: Trang My Packs của ứng dụng

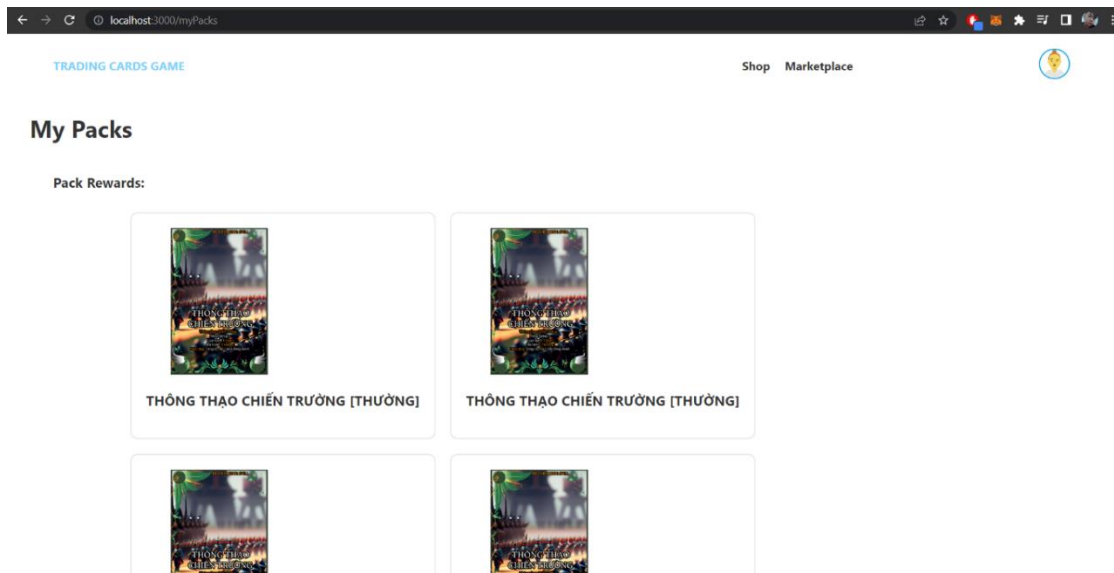
### 2.3.3.2. Mở pack thẻ bài

Tại giao diện này, nhấn vào nút “Open Pack” màu xanh bên dưới những packs thẻ bài mà chúng ta đã mua. Sau đó vài giây hoặc có thể lên đến vài phút sẽ có cửa sổ ví điện tử popup và yêu cầu chúng ta xác nhận giao dịch mở packs thẻ bài (tốn gas nên là sẽ tốn một lượng coin nhỏ chi trả cho số gas). Ta nhấn “Confirm” để mở packs thẻ bài.



Hình 2.3.3.2.1: Mở pack WARRIOR SPELL PACK và xác nhận giao dịch

Sau khi mở packs, trang sẽ hiển thị cho chúng ta những thẻ bài đã nhận được từ việc mở pack vừa rồi:



Hình 2.3.3.2.2: Phần thưởng nhận được sau khi mở pack WARRIOR SPELL PACK



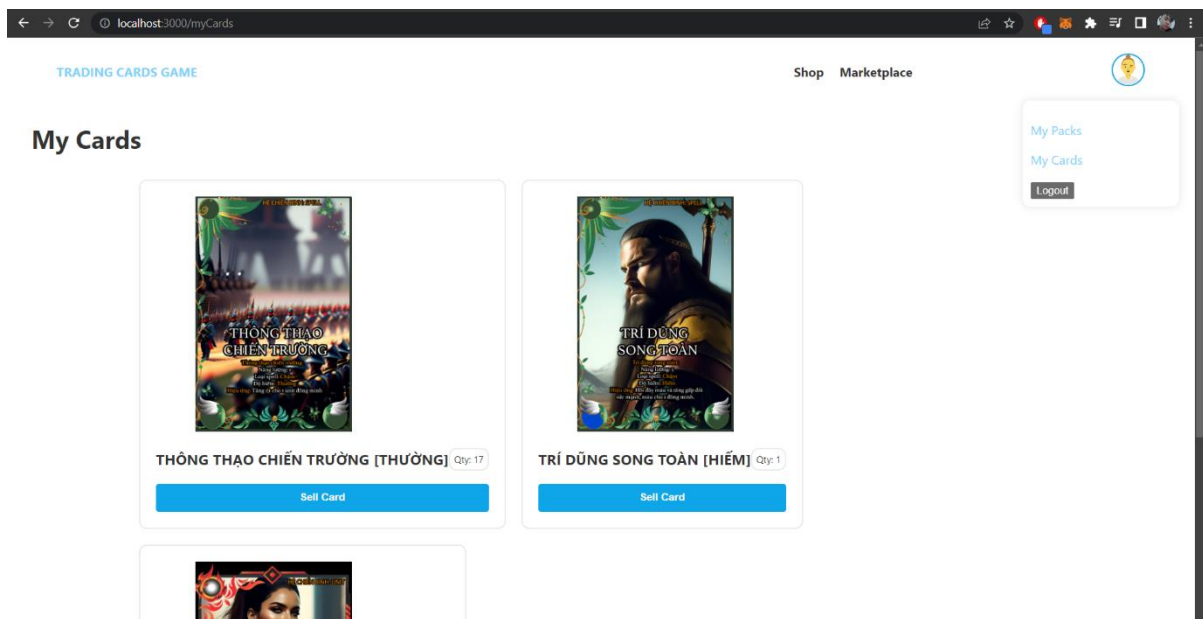
## 2.4.Rao bán thẻ bài đã sở hữu

### 2.4.1.Truy cập vào My Cards

Để tiến hành rao bán thẻ bài của chúng ta, trước tiên chúng ta cần phải truy cập vào trang My Cards để xem những thẻ bài mà chúng ta đã và đang sở hữu.

Để truy cập vào trang My Cards, click vào nút tròn nhỏ với hình avatar người dùng ở phía góc trên bên trái giao diện chương trình.

Sau đó sẽ có một cửa sổ nhỏ sổ ra, trong đó có một vài dòng chữ và một trong số đó là “My Cards” với màu xanh. Click vào dòng chữ này, ứng dụng sẽ điều hướng chúng ta sang trang My Cards của ứng dụng.



Hình 2.4.1: Trang My Cards của ứng dụng

### 2.4.2.Rao bán thẻ bài đã sở hữu

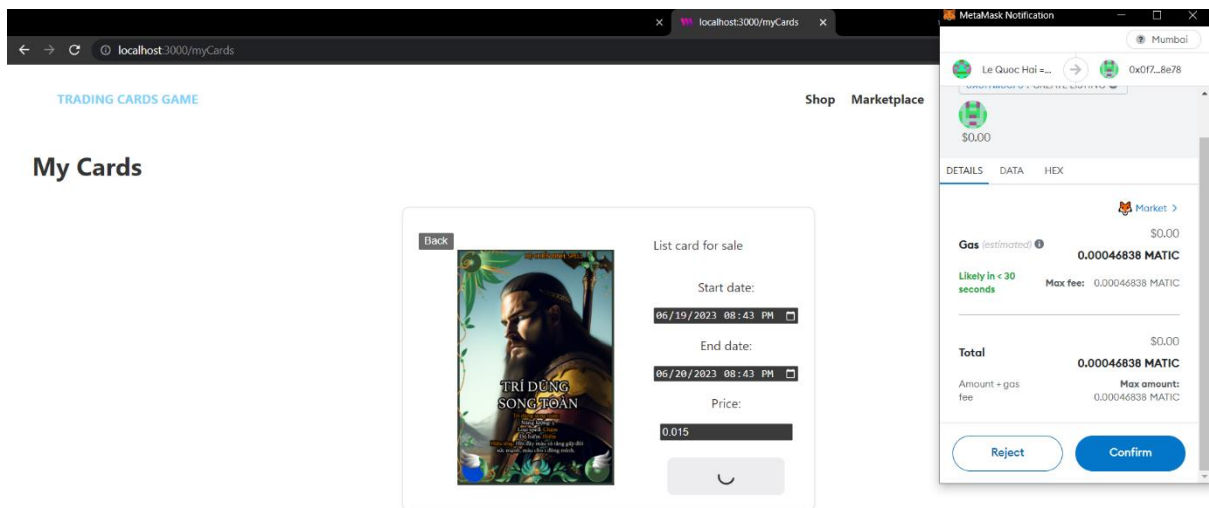
Ở giao diện My Cards, sau khi chúng ta đã xác định được muốn rao bán thẻ bài nào. Chúng ta nhấn vào nút “Sell Card” hình chữ nhật màu xanh ngay bên dưới thẻ bài mà chúng ta muốn rao bán trên thị trường marketplace.

Sau khi click vào nút “Sell Card” như đã nêu trên, sẽ có một cửa sổ nhỏ hình chữ nhật hiện ra và yêu cầu chúng ta chọn Start Date (Ngày bắt đầu rao bán), End date (Ngày kết thúc, không bán nữa), Price (Giá rao bán bằng tiền ảo).

Ta tiến hành nhập đầy đủ thông tin vào và nhấn vào nút “List For Sale” màu xám phía góc phải bên dưới cửa sổ nhỏ.

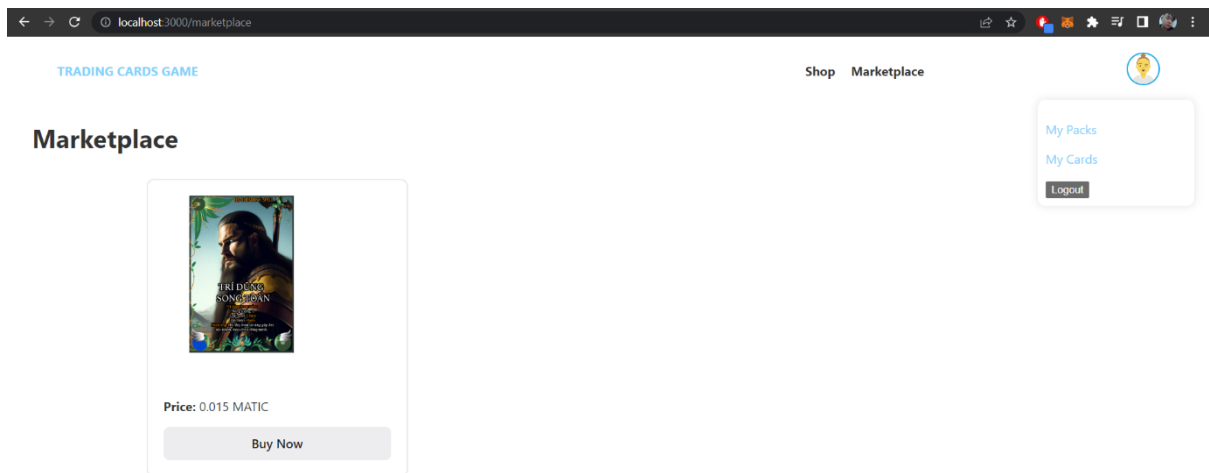
Một lúc sau sẽ có một cửa sổ popup của ví hiện lên và yêu cầu người dùng xác nhận giao dịch. Ta sẽ nhấn vào nút “Confirm”.





Hình 2.4.2.1: Rao bán thẻ bài NFT và xác nhận giao dịch

Sau khi rao bán thành công, ứng dụng sẽ điều hướng chúng ta sang trang marketplace (thị trường giao dịch thẻ bài). Nơi chúng ta có thể mua những thẻ bài của người khác và xem những thẻ bài mà chúng ta đã rao bán.



Hình 2.4.2.2: Rao bán thẻ bài NFT thành công và chuyển hướng sang trang Marketplace

## 2.5. Mua thẻ bài NFT thông qua marketplace

### 2.5.1. Đăng nhập vào ví khác

Ở trên là chúng ta đã rao bán thẻ bài của chúng ta với giá 0.015 MATIC và bây giờ chúng ta sẽ đăng nhập vào một ví khác và tiến hành mua thử nghiệm.

(Tiến hành đăng nhập vào một ví khác như 2.2)

### 2.5.2. Truy cập vào trang marketplace

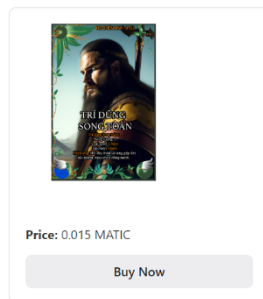
Sau khi đăng nhập vào một ví tiền điện tử khác. Ta tiến hành truy cập vào trang marketplace bằng cách click vào dòng chữ “Market Place” được in đậm trên thanh nền trắng phía góc trên giao diện trang web chúng ta.

TRADING CARDS GAME

Shop Marketplace



#### Marketplace



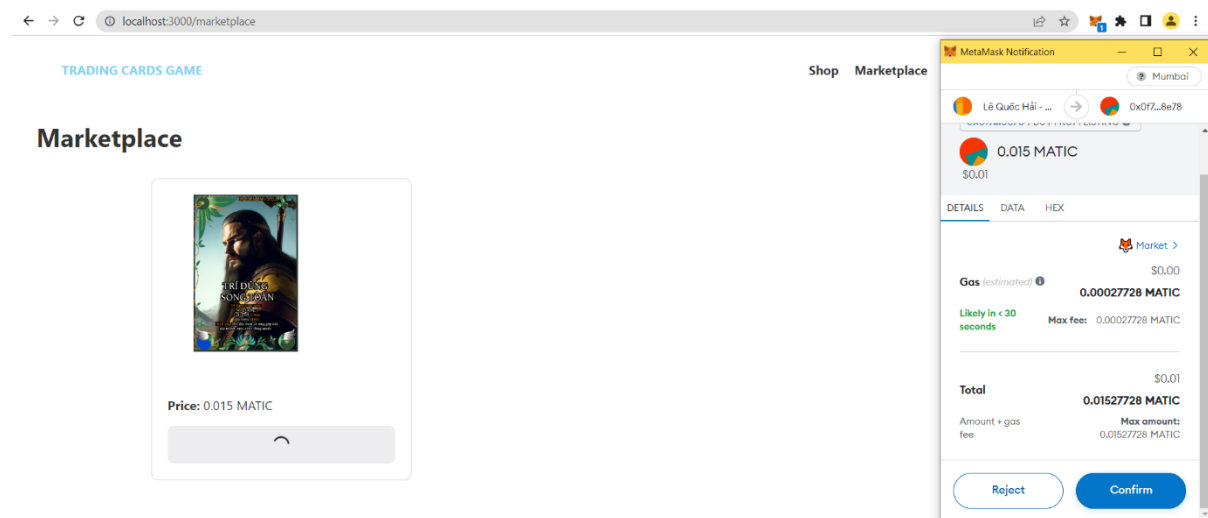
Hình 2.5.2: Trang Marketplace của ứng dụng (truy cập từ một tài khoản khác)

### 2.5.3. Mua thẻ bài từ marketplace

Ở trang marketplace bây giờ, chúng ta click vào nút “Buy Now” màu xám ngay bên dưới thẻ bài mà chúng ta muốn mua.

Sau đó khoảng một vài giây hoặc có thể lên đến một vài phút tùy vào đường truyền, sẽ có một cửa sổ popup của dịch vụ ví tiền điện tử chúng ta sử dụng hiện lên và yêu cầu chúng ta xác nhận giao dịch để tiến hành mua thẻ bài này.

Ta sẽ nhấn vào nút “Confirm” để tiến hành xác nhận giao dịch này và mua lấy thẻ bài này.



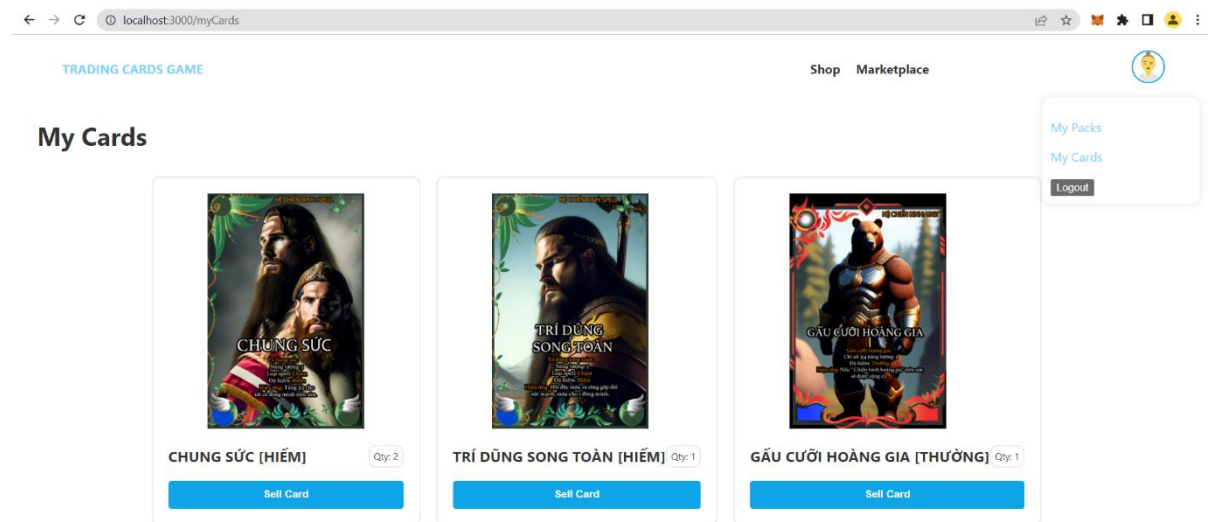
Hình 2.5.3: Mua thẻ bài NFT từ marketplace và xác nhận giao dịch

#### 2.5.4. Truy cập vào trang My Cards để kiểm tra thẻ đã mua

Sau khi mua thẻ bài từ marketplace, thẻ bài mà chúng ta đã dành tiền ra thanh toán đó sẽ thuộc về chúng ta và chúng ta sẽ thấy được nó ở trang My Cards.

Giờ, chúng ta hãy thử truy cập vào My Cards để kiểm tra xem chúng ta đã mua thành công thẻ bài kia chưa nhé!

(Hướng dẫn truy cập vào My Cards như ở phần 2.4.1)



Hình 2.5.4: Trang My Cards của ứng dụng được truy cập bởi một tài khoản khác

Vậy, như hình trên thì chúng ta cũng đã thấy, thẻ bài “TRÍ DŨNG SONG TOÀN [HIẾM]” hiện tại đã và đang thuộc sở hữu bởi tài khoản thứ hai mà chúng ta tạo rồi.