

HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

Final graduation research 1 report

Giảng viên:

Prof. Đào Thành Chung

Sinh viên:

Le Dinh Huy – 20194776

Trường: Công nghệ thông tin & truyền thông

I. Tiến độ và quá trình học tập, nghiên cứu blockchain

1. Đọc sách mastering bitcoin

- Đầu kì học 2022-2, theo hướng dẫn của thầy em đã đọc cuốn sách “mastering bitcoin” và đã hiểu được cơ bản về blockchain. Cụ thể như sau:

- + Blockchain (chuỗi khối) là một công nghệ lưu trữ và truyền thông tin trong một mạng ngang hàng (peer-to-peer network) mà không cần sự tham gia của bên trung gian. Nó là nền tảng cơ sở dữ liệu phân tán, được xây dựng dựa trên các khối thông tin kết nối với nhau theo một cách tiên bộ và bảo mật.
- + Định nghĩa về account, address, wallet trong blockchain: Trong mạng bitcoin, một account thực chất là một cặp khóa công khai và bí mật được lưu trữ trong ví (wallet) người dùng. Address được tạo ra từ khóa công khai (public key) và wallet là phần mềm dùng để lưu trữ, quản lí khóa và thực hiện các giao dịch
- + Block là một cấu trúc dữ liệu dạng container, gom các giao dịch đưa vào blockchain, gồm có header và các giao dịch
- + Transaction là quá trình chuyển tiền từ tài khoản này đến tài khoản khác trong mạng blockchain. Transaction gồm có đầu ra (outputs) và đầu vào (inputs). Yếu tố cơ bản của giao dịch là đầu ra là các UTXO (unspent transaction output)
- + Cơ chế đồng thuận: proof of work (PoW), proof of stake (PoS)...
- + Mining block: 1 node trong mạng sẽ gom các transaction trong mempool vào 1 block ứng cử, node này sẽ tìm giá trị băm header của block ứng cử thỏa mãn yêu cầu về target (trong PoW), khi node tạo ra block mới nó sẽ phát tán lên mạng và các node khác sẽ xác nhận và quá trình đào lại tiếp tục
- + Coin là đơn vị tiền tệ kỹ thuật số được dùng để thực hiện giao dịch trên mạng blockchain, được quản lí và xác định bởi giao thức của mạng blockchain đó
- + Blockchain node: full node, light node, mining node

- Trong quá trình đọc sách, em cũng có ghi chép lại nội dung trong các chapter của sách, đây là link ghi chép em tổng hợp lại:

https://github.com/ledanghuy1811/mastering_bitcoin_note

2. Học solidity (ngôn ngữ lập trình để viết các smart contract)

- Sau khi đọc xong cuốn sách “mastering bitcoin” em bắt đầu học solidity. Cú pháp của solidity khá giống với các ngôn ngữ khác như C++, Javascript nên em cũng không gặp nhiều khó khăn khi học.

- Sau khi học các phần cơ bản của solidity, em cũng đã viết một số smart contracts như:

- + Lottery smart contract
- + Auction smart contract
- + CrowdFunding smart contract
- + Tìm hiểu về chuẩn ERC20 token
- + Tìm hiểu về chuẩn ERC721 để làm dApp nft collection

II. Xây dựng dApp NFT collection

1. Các tính năng

- Xây dựng web nft collection như web bruh bear, giải thích về NFT và chuẩn ERC-721:

- + NFT (viết tắt của Non-Fungible Token) là một loại tiêu chuẩn mã thông báo (token) tiện ích trên blockchain, trong đó mỗi mã thông báo là duy nhất và không thể thay thế bằng bất kỳ mã thông báo khác.
- + Ứng dụng chính của NFT là trong việc xác định và biểu diễn sự sở hữu của các tài sản số không thể thay đổi như tranh nghệ thuật kỹ thuật số, video, âm nhạc, game, bất động sản ảo, và nhiều loại tài sản số khác

+ Nhờ vào tính duy nhất và không thể thay thế của mỗi NFT, người dùng có thể chứng minh rõ ràng rằng họ sở hữu một phiên bản cụ thể của tài sản số

+ ERC-721 là một tiêu chuẩn tiện ích (standard) trên blockchain Ethereum, được sử dụng để tạo và quản lý các token phi fungible (Non-Fungible Tokens - NFTs). Tiêu chuẩn này định nghĩa các quy tắc và giao thức cho việc tạo ra các NFT, đảm bảo rằng mỗi NFT là duy nhất và không thể thay thế bằng bất kỳ NFT nào khác.

+ Một số điểm chính của tiêu chuẩn ERC-721 bao gồm:

- * Duy nhất và không thể thay thế

- * Xác định quyền sở hữu

- * Giao diện chuẩn

- * Tương tác với NFT

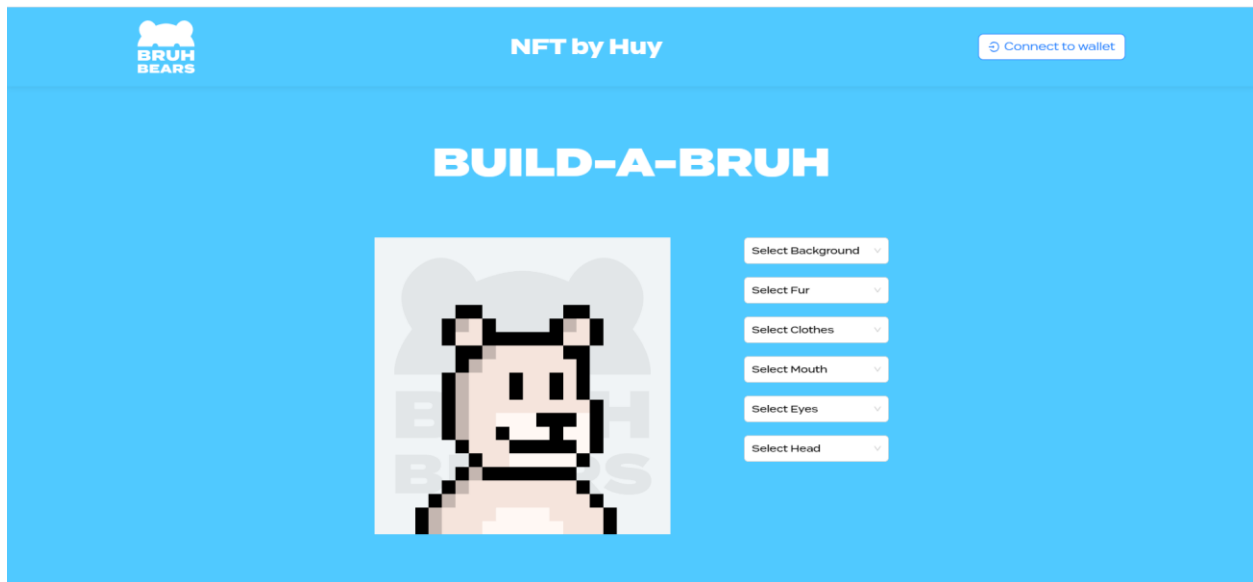
- Công nghệ sử dụng:

+ Viết contract nft sử dụng erc-721: sử dụng thư viện openzeppelin để hỗ trợ viết contract. Deploy contract bằng hardhat

+ Upload ảnh và metadata lên ipfs bằng moralis

+ Tương tác với ví và contract qua wagmi

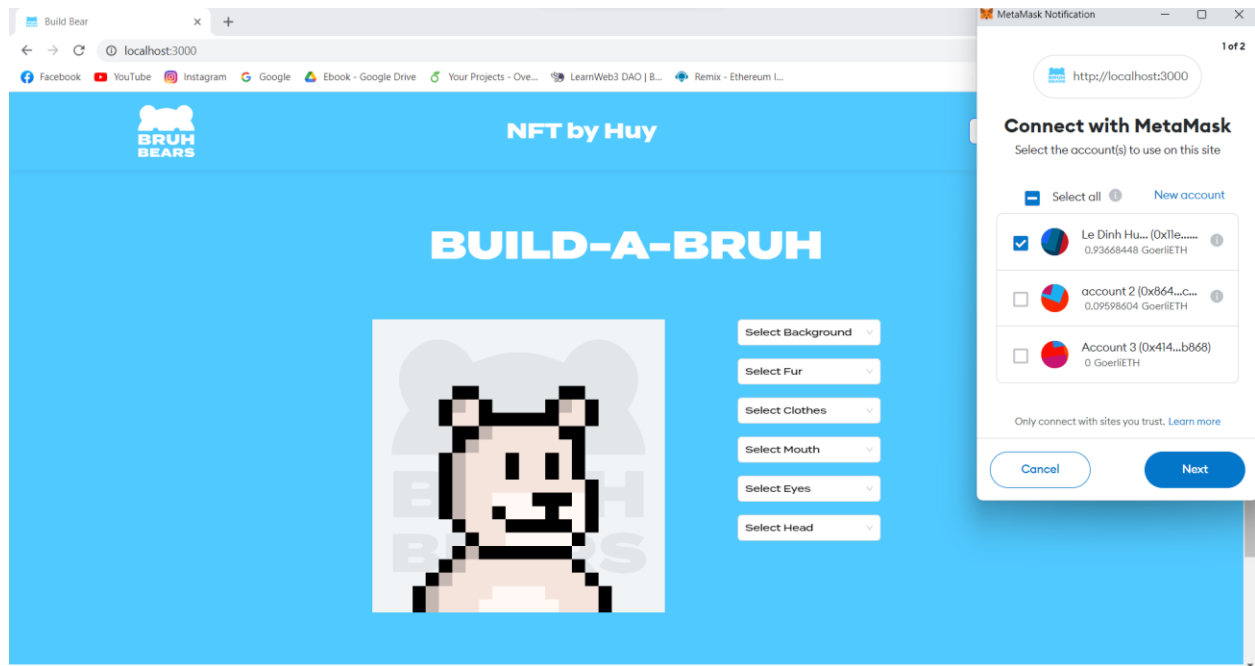
+ UI sử dụng reactjs



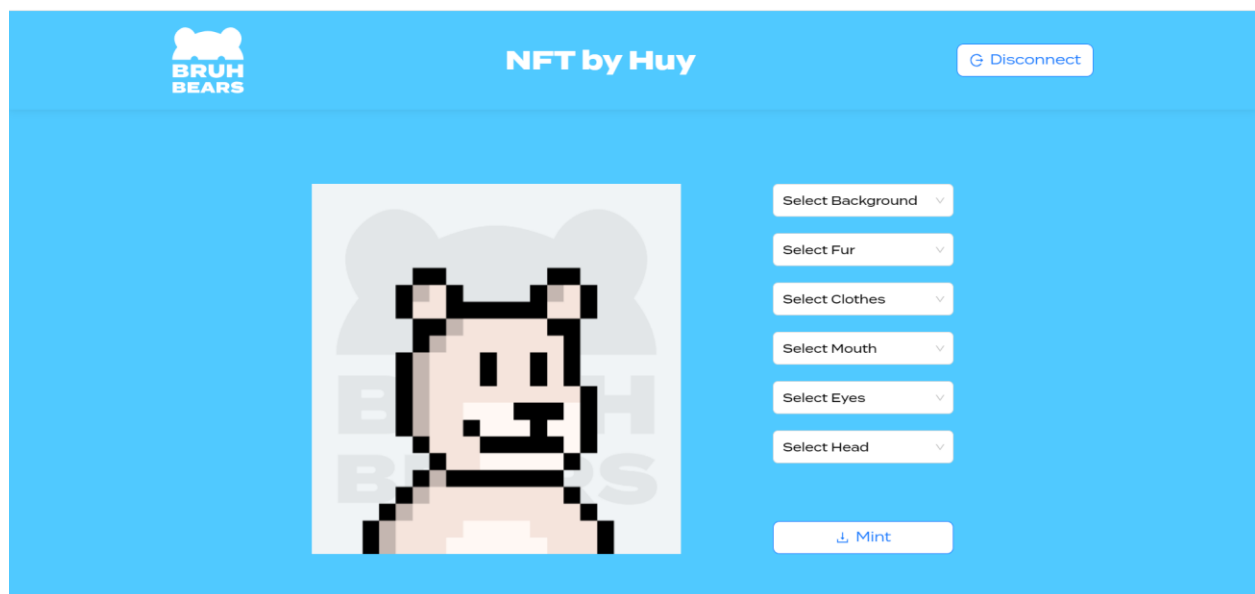
- Đầu tiên người dùng sẽ kết nối với ví metamask để chọn tài khoản kết nối (nếu không kết nối với ví sẽ không mint được nft)
- Sau khi người dùng kết nối với ví thì sẽ thực hiện tạo nft và mint nft:
 - + Người dùng sẽ chọn các tính năng như background, fur, clothes... để tạo ra các nft theo ý thích
 - + Sau đây người dùng sẽ mint nft qua nút mint
- Quá trình mint nft sẽ diễn ra như sau:
 - + Khi người dùng bấm nút mint nft thì sẽ hiện modal xác nhận quá trình:
 - + Đầu tiên sẽ upload ảnh lên ipfs và lấy địa chỉ ảnh đấy
 - + Sau đấy sẽ upload metadata của ảnh bao gồm tên, miêu tả và các thuộc tính, và địa chỉ ipfs của ảnh, sau đấy sẽ lấy ra địa chỉ metadata trả về của ipfs để phục vụ mint
 - + Khi xác nhận mint sẽ thấy modal báo mint thành công, sau đấy người dùng có thể xem được transaction và nft trên testnetsopensea

2. Miêu tả các bước thực hiện:

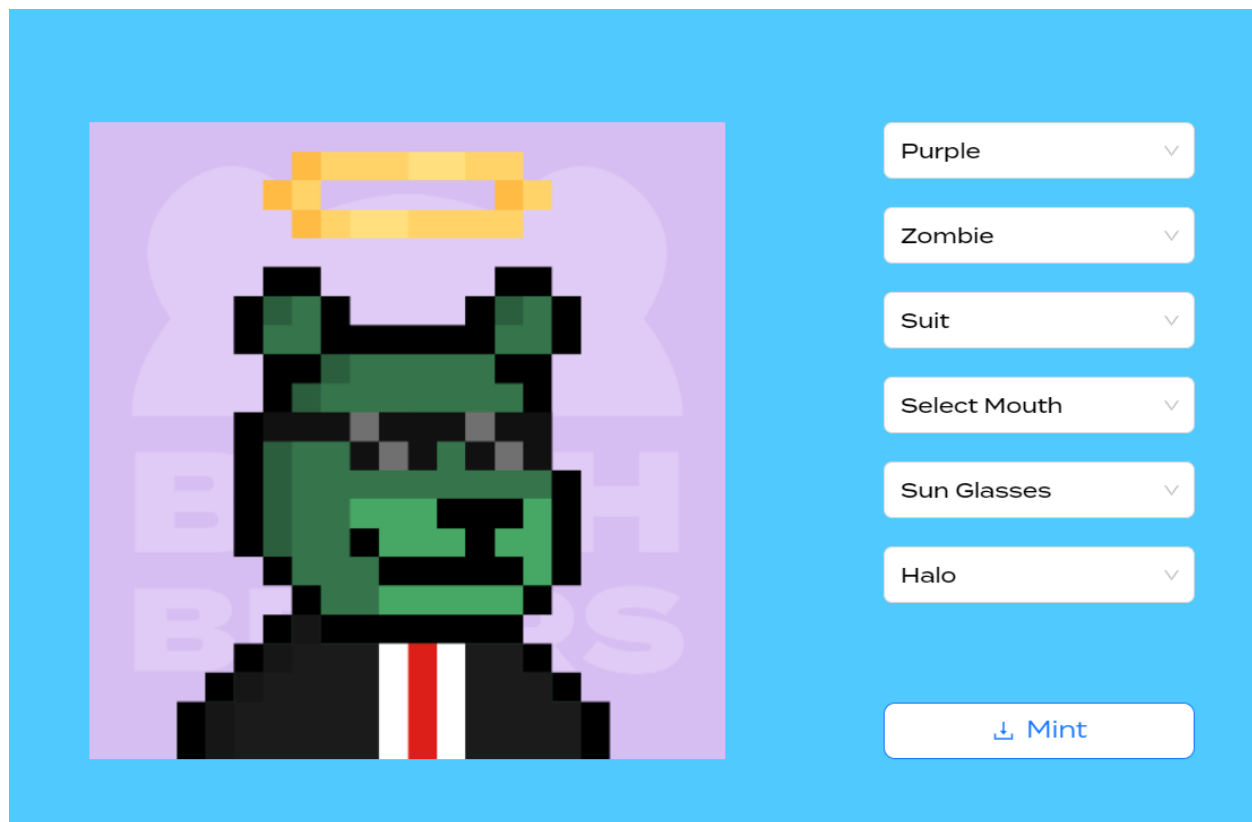
- Đầu tiên người dùng sẽ phải kết nối với ví metamask, khi kết nối xong mới hiện nút mint:



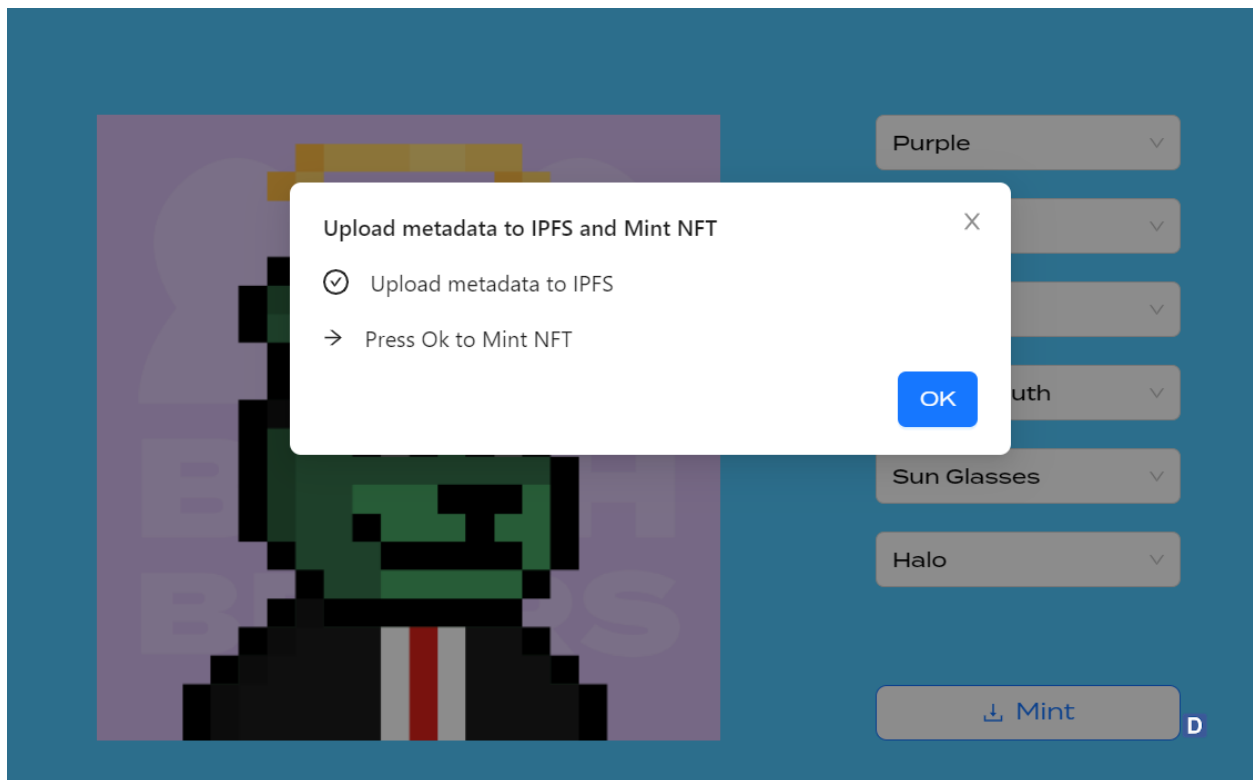
Nút mint:



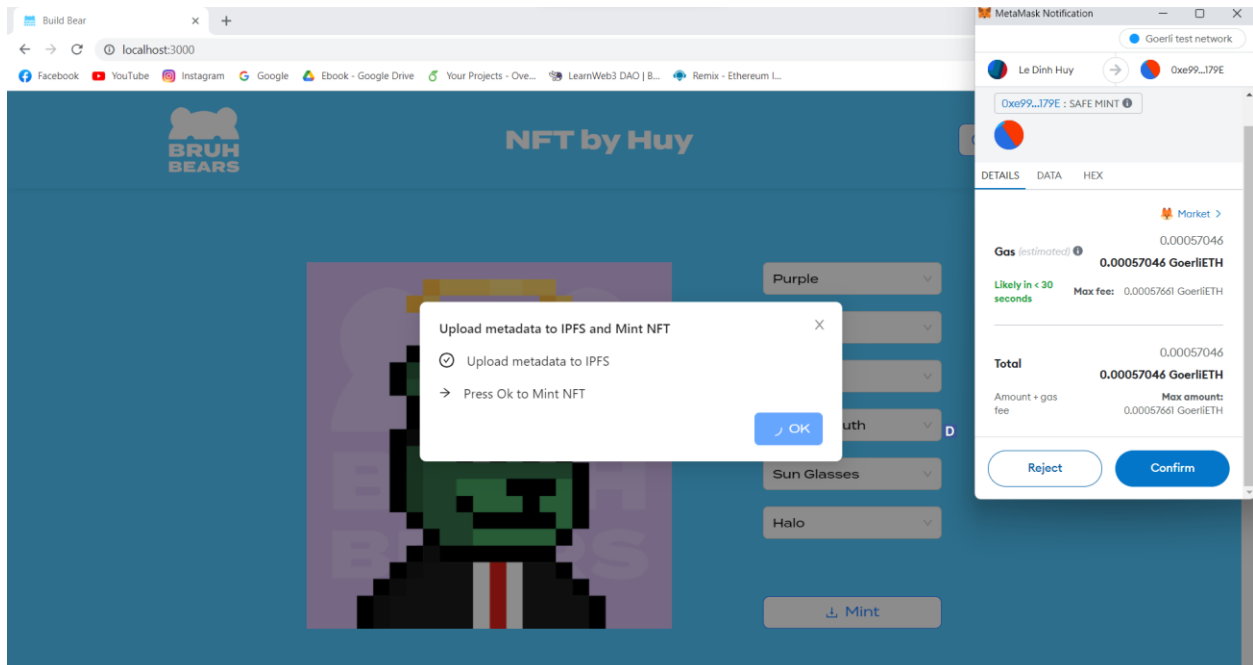
- Sau đây người dùng sẽ thực hiện tạo nft tùy theo ý thích:



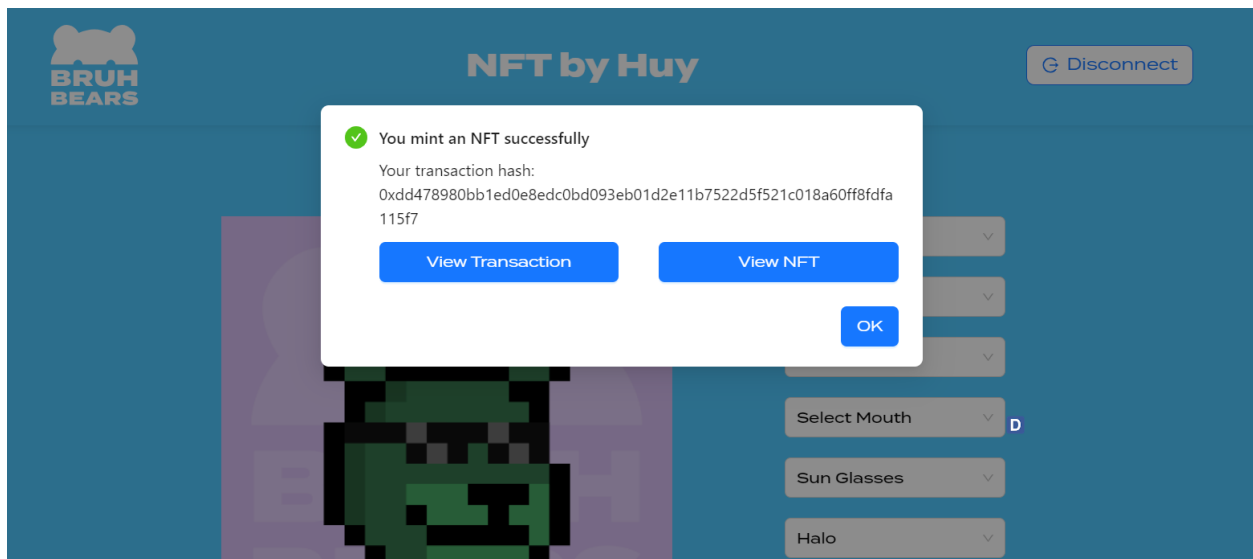
- Sau đây sẽ mint nft:



Xuất hiện modal thông báo, nếu muốn mint sẽ nhấn ok xác nhận:

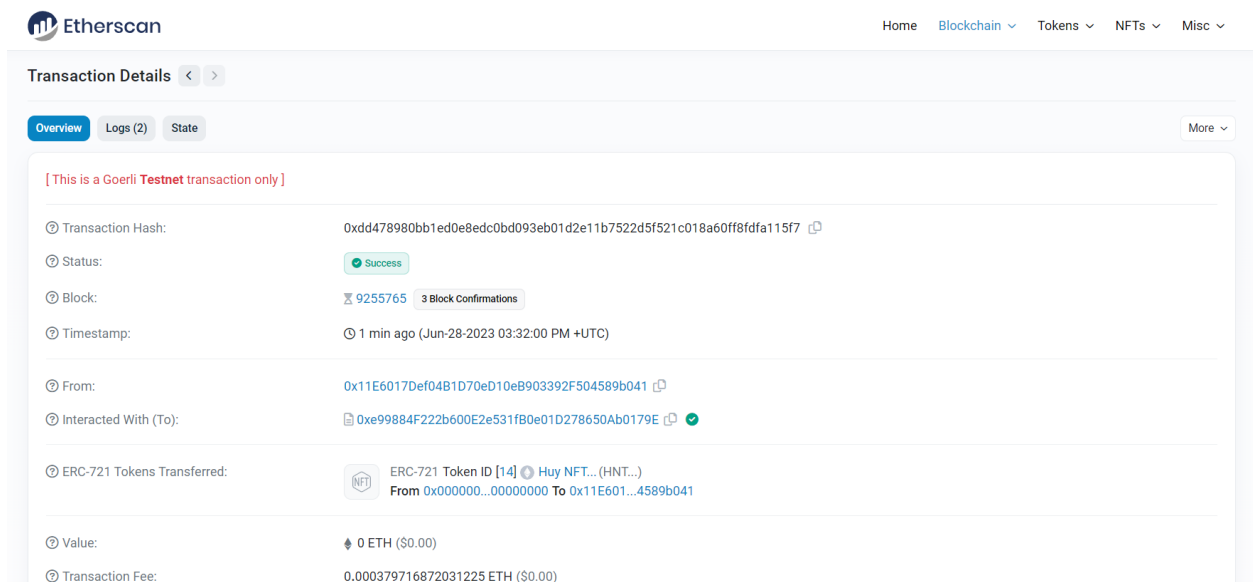


Confirm để mint và chờ. Sau khi mint xong sẽ hiện modal:

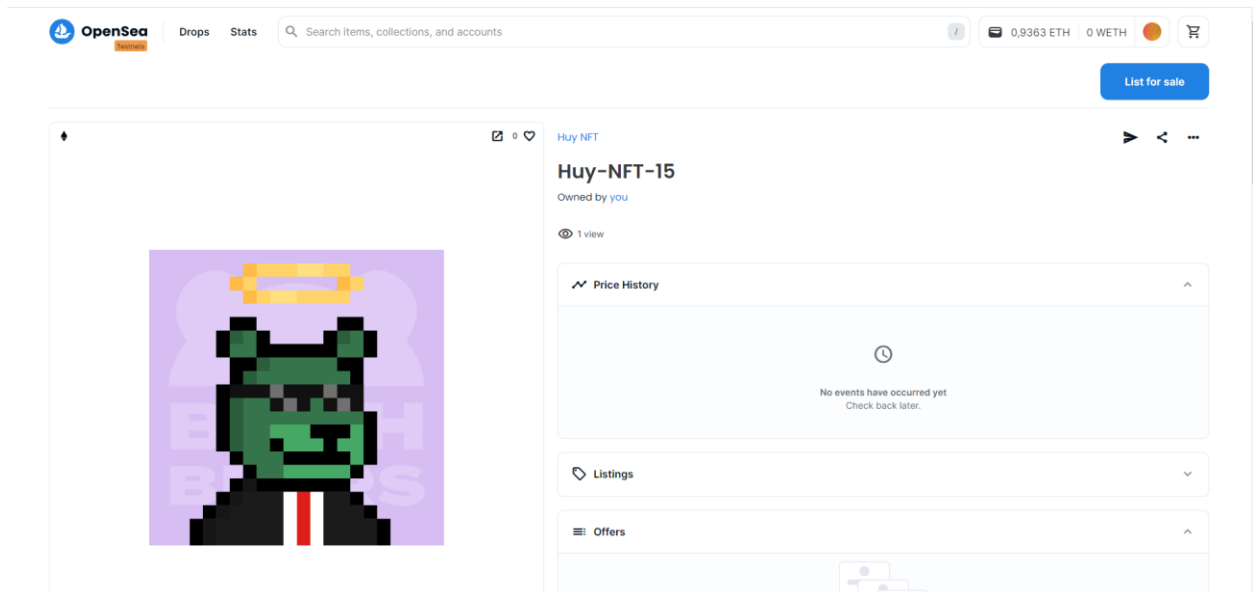


Nếu muốn xem transaction hay nft người dùng sẽ click vào button tương ứng:

- Xem transaction:



- Xem nft:



- Người dùng có thể tiếp tục tạo và mint nft khác nếu muốn
- Nếu người dùng không muốn mint có thể disconnect với ví và nút mint sẽ k còn cho đến khi người dùng kết nối lại:

