|  |  |
| --- | --- |
| **HỌC VIỆN KỸ THUẬT QUÂN SỰ**  **LÊ PHÚ LONG**  **KHÓA 17**  **HỆ ĐÀO TẠO CỬ NHÂN DÂN SỰ**  **KHÓA LUẬN**  **TỐT NGHIỆP ĐẠI HỌC**  **CHUYÊN NGÀNH: KHOA HỌC MÁY TÍNH**  **XÂY DỰNG HỆ THỐNG LAUNCHPAD IDO**  **TRÊN NỀN TẢNG EVM**  **HÀ NỘI, NĂM 2022**  **HỌC VIỆN KỸ THUẬT QUÂN SỰ**  **LÊ PHÚ LONG**  **KHÓA 17**  **HỆ ĐÀO TẠO CỬ NHÂN DÂN SỰ**  **KHÓA LUẬN**  **TỐT NGHIỆP ĐẠI HỌC**  **CHUYÊN NGÀNH: CÔNG NGHỆ THÔNG TIN**  **XÂY DỰNG HỆ THỐNG LAUNCHPAD IDO**  **TRÊN NỀN TẢNG EVM**    ***Cán bộ hướng dẫn: Thượng tá, PGS, TS. Tạ Minh Thanh***   |  | | --- | | **Hà Nội, 2022** | |

|  |  |
| --- | --- |
| **HỌC VIỆN KỸ THUẬT QUÂN SỰ**  **KHOA CÔNG NGHỆ THÔNG TIN BỘ MÔN KHOA HỌC MÁY TÍNH** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

**NHIỆM VỤ KHÓA LUẬN TỐT NGHIỆP**

Họ và tên: Lê Phú Long – KHMT17 - 18150024

Ngành: Khoa học máy tính, Chuyên ngành: Khoa học dữ liệu

1. **Tên đề tài:**

Xây dựng hệ thống launchpad IDO trên nền tảng EVM

**2. Các số liệu ban đầu:**

- Quyết định Giao khóa luận tốt nghiệp đại học – Học viện KTQS

- Tài liệu tham khảo

1. **Nội dung bản thuyết minh**

- Lời nói đầu

- Chương 1: Nghiên cứu lý thuyết lập trình blockchain trên tài liệu có được

- Chương 2: Các khái niệm được nhắc tới và sử dụng bài luận

- Chương 3: Xây dựng chương trình Demo

- Chương 4: Hướng phát triển

- Tổng hợp

- Kết luận

- Tài liệu tham khảo

**4. Số lượng, nội dung các bản vẽ** (ghi rõ loại, kích thước và cách thực hiện các bản vẽ) và các sản phẩm cụ thể (nếu có):

Được sử dụng máy tính và máy chiếu để trình chiếu.

**5. Cán bộ hướng dẫn:**

- Họ và tên: Tạ Minh Thanh

- Học hàm, học vị: Thượng tá, PGS. TS

- Đơn vị: Khoa Công nghệ thông tin

- Hướng dẫn toàn bộ

Ngày giao: 30/06/2022 Ngày hoàn thành: 05/09/2022

*Hà Nội, ngày 05 tháng 09, năm 2022*

**Chủ nhiệm bộ môn Cán bộ hướng dẫn**

(Ký, ghi rõ họ tên, học hàm, học vị)

**Học viên thực hiện**

Đã hoàn thành và nộp khóa luận ngày 05 tháng 09 năm 2022

(Ký và ghi rõ họ tên)

Lê Phú Long

**DANH MỤC HÌNH VẼ**

Hình 1: Thông tin Block…………………………………………………………… 6

Hình 2: Liên kết chuỗi khối trong blockchain……………………………………... 7

Hình 3: Sơ đồ biểu diễn EVM……………………………………………………. 19

Hình 4: Sự khác biệt giữa IDO, IEO, ICO……………………………………….. 28

Hình 5: Sơ đồ biểu diễn thanh khoản…………………………………………….. 30

Hình 6: Sơ đồ biểu diễn pool…………………………………………………….. 31

Hình 7: Sơ đồ biểu diễn mối liên hệ liquidity provider và pool…………………. 32

Hình 8: Giao diện Ganache………………………………………………………. 39

Hình 9: PoolModifier.sol………………………………………………………… 40

Hình 10: Contract IDO.sol……………………………………………………… 41

Hình 11: CreateERC20.sol………………………………………………………. 42

Hình 12: Contract Pool.sol………………………………………………………. 43

Hình 13: Contract Pool.sol………………………………………………………. 44

Hình 14: Contract Pool.sol………………………………………………………. 45

Hình 15: Contract USDT.sol…………………………………………………….. 45

Hình 16: Connect contract thông qua web3……………………………………... 46

Hình 17: ConnectWallet sử dụng web3…………………………………………. 47

Hình 18: Hiển thị balance hiện có của token thông qua web3………………….. 47

Hình 19: Giao diện trước khi connect wallet…………………………………… 48

Hình 20: Giao diện sau khi connect wallet……………………………………... 49

Hình 21: Giao diện tạo token…………………………………………………… 49

Hình 22: Giao diện sau khi tạo token thành công………………………………. 50

Hình 23: Giao diện khởi tạo IDO………………………………………………. 51

Hình 24: Giao diện sau khi khởi tạo IDO………………………………………. 52

Hình 25: Account nhà đầu tư đã tạo……………………………………………. 52

Hình 26: Giao diện người dùng khi mua token IDO…………………………… 54

Hình 27: Giao diện khi thực hiện mua token IDO……………………………… 54

Hình 28: Giao diện sau khi mua thành công……………………………………. 55

Hình 29: Hiện thị số lượng USDT sau khi mua token IDO……………………. 55

Hình 30: Số lượng token IDO đã mua…………………………………………. 56

**MỤC LỤC**

[**LỜI NÓI ĐẦU…………………………………………………………………….. 1**](#_30j0zll)

**Chương 1.** [**TỔNG QUAN VỀ BLOCKCHAIN………………………………. 4**](#_3znysh7)

[**1.1. Khái niệm……………………………………………………………… 4**](#_2et92p0)

[**1.2. Thông tin trong Block (khối)…………………………………………. 5**](#_tyjcwt)

[**1.3. Đặc điểm của Blockchain……………………………………………... 6**](#_3dy6vkm)

[**1.4. Phân loại……………………………………………………………….. 7**](#_1t3h5sf)

[**1.5. Cơ chế hoạt động của Blockchain……………………………………. 7**](#_4d34og8)

[**1.6. Ứng dụng thực tiễn của công nghệ Blockchain……………………... 8**](#_2s8eyo1)

**Chương 2.** [**CÁC KHÁI NIỆM ĐƯỢC NHẮC TỚI VÀ SỬ DỤNG………... 10**](#_3rdcrjn)

[**2.1. Giới thiệu về Token………………………………………………….. 10**](#_26in1rg)

[**2.2. Giới thiệu về Dapps (ứng dụng phi tập trung)…………………….. 10**](#_lnxbz9)

[**2.3. Giới thiệu về DEX (sàn giao dịch phi tập trung)…………………... 11**](#_35nkun2)

[**2.4. Giới thiệu về DeFi (nền tài chính phi tập trung)…………………... 16**](#_1ksv4uv)

[**2.5. Giới thiệu về Ethereum……………………………………………… 20**](#_44sinio)

[**2.6. Giới thiệu về Smart Contract……………………………………….. 21**](#_2jxsxqh)

[**2.7. Giới thiệu về Solidity………………………………………………… 23**](#_z337ya)

[**2.8. Giới thiệu về các chuẩn ERC………………………………………. 24**](#_3j2qqm3)

[**2.9. Giới thiệu về IDO và cách hoạt động của IDO…………………… 26**](#_1y810tw)

[**2.10. Giới thiệu về Liquidity Pool……………………………………... 32**](#_4i7ojhp)

[**2.11. Giới thiệu về Launchpad và cách thức hoạt động……………… 35**](#_2xcytpi)

[**2.12. Giới thiệu về framework web3…………………………………... 37**](#_1ci93xb)

**Chương 3.** [**XÂY DỰNG HỆ THỐNG LAUNCHPAD IDO………………... 41**](#_qsh70q)

[**TRÊN NỀN TẢNG EVM…………………………………………………….. 41**](#_3as4poj)

[**3.1. Tổng quan về ứng dụng………………………………………………... 41**](#_1pxezwc)

[**3.2. Các phần chính của ứng dụng……………………………………….... 41**](#_49x2ik5)

[**3.3. Xây dựng mạng Blockchain………………………………………….... 42**](#_2p2csry)

[**3.4. Lập trình Smart Contract……………………………………………... 43**](#_147n2zr)

[**3.5: Lập trình Web3js………………………………………………………. 49**](#_3o7alnk)

[**3.6. Lập trình giao diện…………………………………………………….. 51**](#_23ckvvd)

[**KẾT LUẬN……………………………………………………………………. 61**](#_ihv636)

[**TÀI LIỆU THAM KHẢO……………………………………………………. 63**](#_2grqrue)

# LỜI NÓI ĐẦU

1. **Sơ lược đề tài**

**Blockchain** là công nghệ cơ sở dữ liệu sáng tạo, trung tâm của gần như tất cả các loại tiền điện tử. Bằng cách phân phối các bản sao giống hệt nhau của cơ sở dữ liệu trên toàn bộ mạng, blockchain làm cho hệ thống rất khó bị hack hoặc gian lận. Mặc dù tiền điện tử đang được sử dụng phổ biến nhất cho blockchain hiện tại nhưng công nghệ này mang lại tiềm năng phục vụ rất nhiều ứng dụng.

Tiền mã hóa đang dần thay thế các loại tiền tệ truyền thống, nhiều người dự đoán rằng đồng tiền này sẽ sớm trở thành một loại tiền tệ toàn cầu. Cơ sở người dùng ngày càng tăng của tiền mã hóa đã cho ra đời nhiều hơn các dự án mới trong lĩnh vực này.

Ngoài ra, nó còn khiến những nhà đầu tư tham gia huy động vốn cộng đồng bằng tiền mã hóa. Chúng ta đều có thể nhận thấy những cơ hội giúp tăng tài sản nhanh chóng khi tham gia vào các chương trình IDO. Và **IDO Launchpad** là một mô hình ra mắt token của một dự án mới trong lĩnh vực tiền điện tử. Ra mắt token lần đầu thường là sự kiện được những nhà đầu tư tiền điện tử chuyên nghiệp luôn chờ đợi. Cách thực hiện IDO Launchpad sẽ nói lên nhiều điều về tương lai liệu một dự án có thành công hay không.

ICO (Cung cấp tiền xu ban đầu) là một trong những mô hình ra mắt token đầu tiên được sử dụng. Khái niệm này được sử dụng vào năm 2013 và trở nên phổ biến vào khoảng năm 2017. Mô hình ICO ban đầu có hiệu quả nhưng nhanh chóng trở nên không khả thi và thiếu tổ chức. Một số nhà đầu tư đã mất tiền vào các dự án lừa đảo như Bitconnect và toàn bộ “Hệ thống ủy thác” của ICO đã sụp đổ.

Có nhiều mô hình ra mắt token khác nhau sau mô hình ICO, chẳng hạn như Niêm yết lần đầu trên [Uniswap](https://vn.beincrypto.com/learn/dau-tu-tien-dien-tu-voi-uniswap/) (Initial Uniswap Listing) hay Tạo dựng thanh khoản Balancer (Balancer Liquidity Bootstrapping). Những phương thức này cũng đã được cường điệu hóa trong một thời gian.

Tuy nhiên, các mô hình ra mắt token mới đã thay đổi đáng kể trong những năm gần đây, với mô hình phát hành DEX lần đầu (IDO) đã khôi phục lại niềm tin “đã mất” vào các phương pháp cấp vốn tiền điện tử trước đây.

1. **Mục đích nghiên cứu**

- Mong muốn tìm hiểu sâu hơn cách hoạt động và các ứng dụng của Blockchain

- Nghiên cứu cách hoạt động trong quá trình gọi vốn đầu tư

Do quá trình làm đồ án còn hạn chế về thời gian và kinh nghiệm, em mong nhận được những góp ý chân thành từ thầy cô.

1. **Phạm vi nghiên cứu**

Đề tài xây dựng hệ thống launchpad IDO trên nền tảng EVM, cụ thể là nghiên cứu quy trình gọi vốn trên hệ thống launchpad, cách IDO các token và cách nó hoạt động từ tạo token cho đến IDO token đó và giao dịch mua bán token.

1. **Kết cấu của đồ án**

**-** Mở đầu:

Trình bày lý do chọn đề tài, mục tiêu, phạm vi nghiên cứu, bố cục luận án.

**-** Chương I: Tổng quan về Blockchain

Chương này giới thiệu về tổng quan về Blockchain, khái niệm, đặc điểm, cơ chế hoạt động và ứng dụng của Blockchain

- Chương II: Các khái niệm được nhắc tới và sử dụng trong bài luận

Đây là những khái niệm cơ bản và buộc phải nắm bắt và hiểu rõ. Từ đó mới có thể hiểu rõ công việc chúng ta đang làm.

- Chương III: Xây dựng hệ thống launchpad IDO trên nền tảng EVM

Chương này, giới thiệu về sản phẩm demo. Một dapp cho phép IDO các token.

- Kết luận:

Phần này đánh giá kết quả mà khóa luận đạt dược cũng như những thiếu sót và những định hướng trong tương lai

## Chương 1

## TỔNG QUAN VỀ BLOCKCHAIN

#### 1.1. Khái niệm

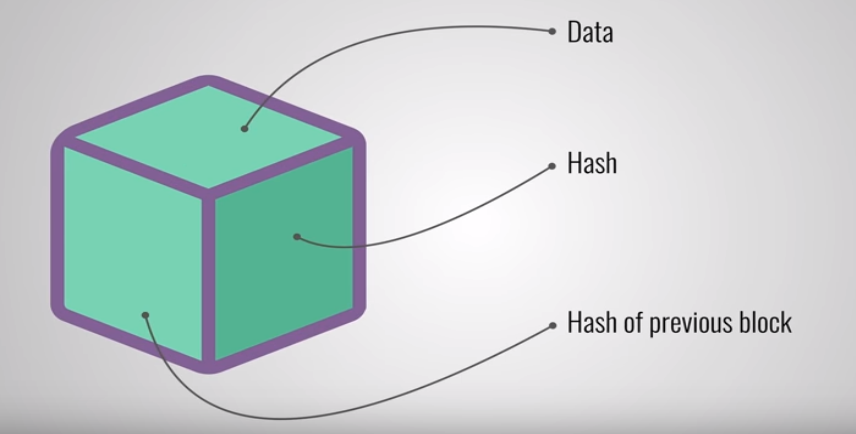
Blockchain (hay cuốn sổ cái) là hệ thống cơ sở dữ liệu cho phép lưu trữ và truyền tải các khối thông tin (block). Chúng được liên kết với nhau nhờ mã hóa.

Các khối thông tin này hoạt động độc lập và có thể mở rộng theo thời gian. Chúng được quản lý bởi những người tham gia hệ thống chứ không thông qua đơn vị trung gian.

Nghĩa là khi một khối thông tin được ghi vào hệ thống Blockchain thì không có cách nào thay đổi được. Chỉ có thể bổ sung thêm khi đạt được sự đồng thuận của tất cả mọi người.

Khối thông tin mà chúng ta đang nhắc đến là những cuộc trao đổi, giao dịch trong thực tế.

#### 1.2. Thông tin trong Block (khối)

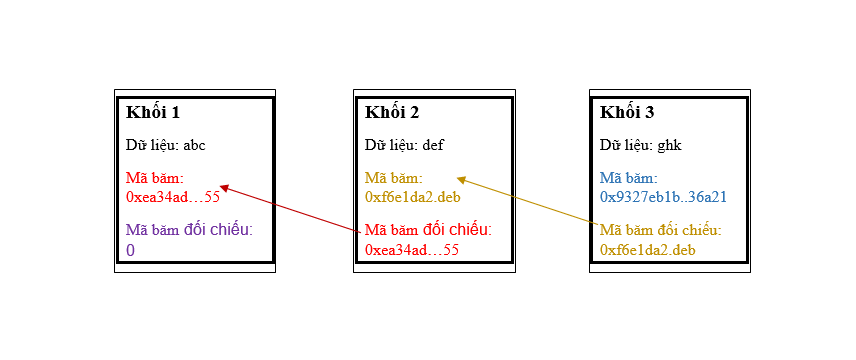


**Hình 1: Thông tin Block**

- Dữ liệu (data). Dữ liệu trong mỗi khối phụ thuộc vào loại blockchain, ví dụ blockchain của bitcoin chứa thông tin về các giao dịch như thông tin người gửi, người nhận tiền và số bitcoin được giao dịch.

- Mỗi khối có một mã băm (Hash) để nhận dạng một khối và các dữ liệu trong đó. Mã này là duy nhất, nó tương tự như dấu vân tay. Bất kỳ sự thay đổi nào trong khối thì mã băm cũng sẽ thay đổi.

- Mã băm đối chiếu (chính là mã của khối phía trước – Hash of previous block) sẽ tạo thành chuỗi. Bất cứ sự thay đổi một khối sẽ khiến các khối tiếp theo không phù hợp.



**Hình 2: Liên kết chuỗi khối trong blockchain**

Từ bất kỳ một khối, ta có thể truy cập tất cả các khối trước đó và các khối tiếp theo trong chuỗi liên kết. Vì vậy, cơ sở dữ liệu trong blockchain lưu trữ lịch sử đẩy đủ và không thể xóa của tất cả các giao dịch được thực hiện từ lần đầu tiên.

#### 1.3. Đặc điểm của Blockchain

- Không thể làm giả, không thể phá hủy các chuỗi Blockchain: theo như lý thuyết thì chỉ có máy tính lượng tử mới có thể giải mã Blockchain và công nghệ Blockchain biến mất khi không còn Internet trên toàn cầu.

- Bất biến: dữ liệu trong Blockchain không thể sửa (có thể sửa nhưng sẽ để lại dấu vết) và sẽ lưu trữ mãi mãi.

- Bảo mật:  Thông tin, dữ liệu trong Blockchain được phân tán và an toàn tuyệt đối.

- Minh bạch: Ai cũng có thể theo dõi dữ liệu Blockchain đi từ địa chỉ này tới địa chỉ khác và có thể thống kê toàn bộ lịch sử trên địa chỉ đó.

- Hợp đồng thông minh: là hợp đồng kỹ thuật số được nhúng vào đoạn code if-this-then-that (IFTTT), cho phép chúng tự thực thi mà không cần bên thứ ba.

#### 1.4. Phân loại

Có cả blockchain Public (công khai) và Private (riêng tư).

Trong một **blockchain công khai**, bất kỳ ai cũng có thể tham gia, nghĩa là họ có thể đọc, viết hoặc kiểm tra dữ liệu trên blockchain. Rất khó để thay đổi các giao dịch được đăng nhập trong một blockchain công khai vì không có cơ quan quyền lực duy nhất nào kiểm soát các node của blockchain.

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

#### 1.5. Cơ chế hoạt động của Blockchain

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

Cách các khối mới này được tạo ra là chìa khóa giải thích tại sao blockchain được coi là an toàn cao. Phần lớn các node phải xác minh và xác nhận tính hợp pháp của dữ liệu mới trước khi một khối mới có thể được thêm vào sổ cái kỹ thuật số.

Đối với tiền điện tử, chúng có thể liên quan đến việc đảm bảo rằng các giao dịch mới trong một khối không phải là gian lận hoặc tiền chưa được sử dụng nhiều hơn một lần. Điều này khác với cơ sở dữ liệu hoặc bảng tính độc lập, nơi một người có thể thực hiện các thay đổi mà không cần giám sát.

Sau khi có sự đồng thuận, khối sẽ được thêm vào chuỗi và các giao dịch cơ bản được ghi lại trong sổ cái phân tán. Các khối được liên kết với nhau một cách an toàn, tạo thành một chuỗi kỹ thuật số an toàn từ đầu cho tới cuối sổ cái. Các giao dịch thường được bảo mật bằng mật mã, có nghĩa là các node cần giải các phương trình toán học phức tạp để xử lý một giao dịch.

#### 1.6. Ứng dụng thực tiễn của công nghệ Blockchain

Một số ngành công nghiệp mà công nghệ Blockchain có thể**tác động** đến như:

- Công nghệ ô tô Automotive (Automotive)  
- Chế tạo (Manufacturing)  
- Công nghệ, truyền thông và viễn thông (Tech, media & Telecommunications)  
- Dịch vụ tài chính (Financial Services)  
- Nghệ thuật & Giải trí (Art & Recreation)  
- Chăm sóc sức khỏe (Healthcare)  
- Bảo hiểm (Insurance)  
- Bán lẻ (Retail)  
- Bất động sản (Property)  
- Nông nghiệp (Agricultural)  
- Khai thác (Mining)  
- Vận tải và Logistics (Transport & Logistics)  
- Công trình hạ tầng kỹ thuật (Utility)

## Chương 2

## CÁC KHÁI NIỆM ĐƯỢC NHẮC TỚI VÀ SỬ DỤNG

#### 2.1. Giới thiệu về Token

**Token** là một loại tài sản điện tử được phát hành và hoạt động trên nền tảng Blockchain của các dự án có sẵn nhờ tạo ra các Smart Contract mà không sở hữu Blockchain riêng.

Phổ biến nhất phải kể đến Ethereum. Mã thông báo của Token được xây dựng trên nền tảng Ethereum thông thường sẽ là chuẩn ERC-20.

Token có thể được sử dụng như một phương thức thanh toán trong hệ sinh thái của dự án.

#### 2.2. Giới thiệu về Dapps (ứng dụng phi tập trung)

1. Khái niệm

- Các ứng dụng phi tập trung (DApps - Decentralized Application) là các phần mềm được triển khai độc lập, không nằm trên một máy chủ duy nhất mà được lưu trữ một cách phân tán trên các kho lưu trữ phi tập trung và có thể được viết bằng bất kỳ ngôn ngữ nào và dưới sự hỗ trợ của Smart Contract.

- Vì các ứng dụng phi tập trung được xây dựng trực tiếp trên các [Blockchain Platform](https://coin98.net/blockchain-platform) (Bitcoin, Ethereum, ….) nên tính chất của các ứng dụng phi tập trung này sẽ phụ thuộc vào các Blockchain Platform đó.

1. Đặc điểm của Dapps

- Đặc điểm chung của các DApp là tính phi tập trung. Do đó không ai có thể kiểm soát được những hoạt động của người dùng trên các dự án này. Ngoài ra, xu hướng của các ứng dụng phi tập trung trong Crypto thường là mã nguồn mở, cộng đồng có thể tạo ra những dự án khác từ bộ code của các ứng dụng phi tập trung cũ.

- Để xây dựng được ứng dụng phi tập trung thì nền tảng Blockchain đó phải có Smart Contract.

- Các ứng dụng phi tập trung thường có chung các bước phát triển,

bao gồm: Lên ý tưởng, xuất bản Whitepaper, tạo token, phân phối token,...

#### 2.3. Giới thiệu về DEX (sàn giao dịch phi tập trung)

**DEX (Decentralized Exchange**)

**2.3.1. Khái niệm:**

Là loại sàn giao dịch tiền điện tử được xây dựng và hoạt động một cách phi tập trung dựa trên nền tảng [blockchain](https://wiki.tino.org/blockchain-la-gi/). Sàn DEX cho phép các người dùng có thể giao dịch mua bán ngang hàng ngay trên mạng lưới blockchain mà không cần phải thông qua bất kỳ tổ chức trung gian nào.

**2.3.2. Đặc điểm:**

* Hệ thống phi tập trung sử dụng một mạng lưới thanh toán ngang cấp (P2P) tự động mà không có sự can thiệp của một tổ chức trung gian nào.
* Lượng tài sản luôn được nắm giữ bởi chủ sở hữu và lưu trữ an toàn trong ví, được bảo mật bởi một khóa duy nhất. Điều này khiến cho DEX trở thành một “hệ thống đáng tin cậy”. Nếu số tiền được nắm giữ hoàn toàn bởi chủ sở hữu sẽ không cần phải tin tưởng vào bên thứ ba.
* Bảo mật thông tin là chìa khóa cũng như bước đột phá của DEX.

**2.3.3. Một số mô hình DEX phổ biến:**

- On-Chain orderbooks (sổ lệnh trên chuỗi)

Mọi giao dịch đều được ghi vào Blockchain. Hệ thống yêu cầu tất cả các node cùng tham gia xác nhận giao dịch. Người dùng phải trả phí cao và chờ đợi khá lâu để các giao dịch được hoàn thành. Bitshares và StellarTem là các sàn áp dụng mô hình này.

- Off-Chain orderbooks (sổ lệnh ngoài chuỗi)

Các lệnh không bị ràng buộc về tốc độ giao dịch và được lưu lại trên một máy chủ tập trung thay vì lưu trên blockchain. Tuy nhiên, bạn đừng quá lo lắng, khi thực hiện giao dịch tại đây vẫn đảm bảo bạn là người có toàn quyền nắm giữ và quản lý tài sản của mình.

So với on-chain orderbook thì sàn DEX mô hình này có tốc độ giao dịch nhanh và phí giao dịch rẻ hơn. Một số sàn áp dụng mô hình này thành công phải kể đến như Binnace DEX, EtherDelta và 0x.

- AMM (Automated Market Makers)

AMM không sử dụng sổ lệnh mà tận dụng các smart contract để tạo ra các nhóm thanh khoản tự động thực hiện giao dịch. AMM tương đối thân thiện với người dùng. Các giao dịch trên DEX AMM được thực thi on-chain nên bạn phải tốn phí. Uniswap, Pancakeswap, Sushiswap… là các sàn DEX AMM phổ biến nhất hiện nay.

- PMM (Proactive Market Maker)

PMM tận dụng Price Oracle giúp giảm trượt giá và mang lại sự ổn định giá tốt hơn AMM. Nhà cung cấp thanh khoản sẽ ít phải chịu rủi ro Impermanent Loss. Bạn có thể trải nghiệm sàn PMM DEX trên DODO Exchange.

- Hybrid Liquidity DEX

Là sự kết hợp các tính năng tốt nhất của orderbook và AMM. Giao dịch được thực hiện tức thì với mức giá tốt nhất và tiết kiệm chi phí hiệu quả. Idex là một trong số ít các sàn áp dụng mô hình này thành công.

**2.3.4. Ưu điểm:**

- Không cần KYC

[KYC](https://wiki.tino.org/kyc-la-gi/) luôn được xem là tiêu chuẩn bắt buộc của nhiều sàn giao dịch. Vì các lý do pháp lý liên quan đến chống rửa tiền, các cá nhân thường phải gửi giấy tờ tùy thân và bằng chứng địa chỉ.

Điều này trở thành là mối quan ngại về tính riêng tư đối với một số người hoặc khá phiền phức khi giấy tờ bạn cung cấp không hợp lệ. Còn với sàn DEX sẽ không cần cấp quyền và không có ai kiểm tra danh tính của bạn. Tất cả bạn cần là một ví tiền điện tử để lưu trữ tài sản.

- Không rủi ro đối tác

Một yếu tố quan trọng khiến các sàn giao dịch phi tập trung ngày càng hấp dẫn là vì chúng không giữ tiền của khách hàng. Tài sản của người dùng đều nằm trên blockchain và được bảo mật bởi các nodes trong mạng lưới.

- Giao dịch các token không phổ biến và không được liệt kê

Người dùng vẫn có thể giao dịch các token không phổ biến và không được liệt kê trên các sàn tập trung một cách thoải mái trên các sàn DEX, miễn có cung và cầu.

**2.3.5. Nhược điểm:**

- Trải nghiệm người dùng của DEX chưa tốt

Mặc dù những sàn DEX mới xuất hiện gần đây đã cải thiện nhất nhiều về trải nghiệm người dùng so với các sàn cũ. Nhưng vẫn chưa thể đáp ứng độ mượt mà giống như các sàn CEX đang thực hiện.

Tuy nhiên, chúng ta có thể hy vọng các sàn phi tập trung sẽ cải tiến hơn trong tương lai gần.

- Khối lượng giao dịch và tính thanh khoản ít

Nếu so sánh trực tiếp với các sàn giao dịch tập trung, khả năng thanh khoản ở các sàn giao dịch phi tập trung đang kém hơn rất nhiều. Điều này xuất phát từ việc người dùng ít sử dụng các sàn DEX do nhiều yếu tố khác nhau. Trong một thị trường có tính thanh khoản kém, bạn sẽ khó tìm thấy người muốn giao dịch với mình ở một mức giá hợp lý.

Ngoài ra, các sàn DEX vẫn còn khá mới mẻ, do đó chưa chắc sẽ có cung và cầu cho các tài sản tiền điện tử mà bạn muốn giao dịch.

- Độ trễ giao dịch

Độ trễ giao dịch cũng là một hạn chế trên các sàn DEX. Vì các lệnh được thực hiện on-chain trên nền tảng blockchain và cần chờ đợi sự xác nhận của các nodes nên dẫn đến độ trễ của lệnh giao dịch được thực hiện.

- Phí

Phí trên các sàn DEX không phải luôn cao nhưng có thể sẽ cao, đặc biệt là khi mạng lưới quá tải và bạn đang sử dụng một sổ lệnh trên chuỗi.

#### 2.4. Giới thiệu về DeFi (nền tài chính phi tập trung)

**DeFi (**[**Decentralized Finance**](https://vi.wikipedia.org/wiki/T%C3%A0i_ch%C3%ADnh_phi_t%E1%BA%ADp_trung)**)**

**2.4.1. Khái niệm:**

- là nền tài chính phi tập trung (hay tài chính mở) mà trong đó, các tổ chức, thị trường hay các công cụ tài chính được quản lý phi tập trung.

- DeFi tận dụng sức mạnh của Blockchain là phi tập trung và minh bạch để tạo nên 1 nền tài chính mở, mà trong đó mọi người đều có thể truy cập và sử dụng nó ở bất kỳ đâu, bất kỳ khi nào mà không chịu sự chi phối bởi cá nhân, tổ chức tập trung quyền lực nào cả.

Trong DeFi luôn đi kèm với “Non-Custodial", tức là không uỷ thác. Cũng nhờ vào đặc điểm này của DeFi mà chúng ta thường gọi nó là Open Finance hay tài chính mở.

**2.4.2. Các tính chất của DeFi:**

DeFi chính là ứng dụng thiết thực nhất của blockchain. Nó tận dụng được các ưu điểm của blockchain.

Bao gồm:

- Tính phi tập trung (Decentralized):

Không có sự tồn tại của tổ chức hay cơ quan chức năng. Người dùng sẽ có toàn quyền kiểm soát tài sản của họ và tương tác với hệ sinh thái qua ứng dụng phi tập trung và ứng dụng ngang hàng.

- Tính minh bạch (Transparent):

Những tác động của con người sẽ được hạn chế. Bởi vì tất cả hoạt động đều được ghi nhận và công khai.

- Không cần sự cho phép (Permissionless):

Tất cả người dùng đều bình đẳng với nhau và không cần đăng ký với thủ tục rườm rà.

- Chi phí thấp:

Bởi vì không có cơ quan hay tổ chức nên mọi chi phí trả cho bên thứ 3 đều được cắt giảm.

- Không cần uỷ thác (Self-Custody):

Người dùng cần uỷ thác cho bên thứ 3. Hiện giờ, người nhận vai trò này là Smart Contract, đồng thời duy trì luật chơi trong thị trường DeFi.

**2.4.3. Ưu điểm:**

- DeFi giúp việc gia nhập thị trường tài chính trở nên dễ dàng hơn:

Ở DeFi việc tín nhiệm hoàn toàn là điều không cần thiết. Bạn không cần phải chứng minh danh tính hay khả năng hoàn trả khoản vay của mình. Luật chơi được đưa ra và các bên phải tuân theo luật chơi đó. Và lúc này, smart contract chính là trọng tài giúp duy trì luật chơi và đảm bảo quyền lợi của các bên.

- Không cần các tổ chức trung gian:

Với công nghệ blockchain đứng sau để “chống lưng”, DeFi loại bỏ được yếu tố trung gian như ngân hàng hay Chính phủ. Lúc này bất kỳ ai cũng có thể tiếp cận được với các sản phẩm dịch vụ về tài chính mà không cần phải được sự cho phép và quản lý bởi các cơ quan này.

- DeFi đẩy giá crypto lên cao:

Kể từ khi DeFi ra đời, giá trị vốn hóa thị trường của các dự án lớn trong phân khúc đã tăng lên đáng kể. Giá một số đồng coin thậm chí đã tăng gấp đôi trong vòng chưa đầy một năm.

- Tăng tính toàn diện hơn của các dịch vụ tài chính:

Bằng cách cung cấp các công cụ tự động cho tất cả mọi người, với việc thực hiện minh bạch và không phân biệt đối xử.

**2.4.4. Nhược điểm:**

- Khả năng mở rộng, thông lượng và phí giao dịch:

 Cho các nền tảng thanh toán blockchain còn hạn chế. Việc sử dụng năng lượng còn làm dấy lên lo ngại về việc góp phần làm biến đổi khí hậu.

- Tính hợp pháp chưa được công nhận:

Bản thân DeFi hay thậm chí là công nghệ blockchain vẫn còn đang là một dấu hỏi lớn hiện nay. Tại nhiều quốc gia trên thế giới, blockchain và các sản phẩm của nó vẫn chưa được xem là hợp pháp. Điều này có nghĩa là nếu có bất kỳ tranh chấp nào xảy ra, sẽ không có ai bảo lãnh hay giải quyết cho bạn cả.

- Tính thanh khoản kém:

Thị trường DeFi hiện tại vẫn không thể lớn như các hệ thống tài chính truyền thống. Vì vậy, có thể khó đặt niềm tin của người dùng vào một lĩnh vực không mang lại nhiều lợi nhuận như lĩnh vực tài chính thông thường.

- Rủi ro về vấn đề tập trung hoá:

Blockchain không thể truy cập thông tin ngoài chuỗi. Vì vậy, cần có bên thứ ba cung cấp dữ liệu trong thế giới thực cho blockchain, điều này làm cho dữ liệu bị tập trung hóa và dễ bị ảnh hưởng bởi các vấn đề liên quan đến tập trung.

- Các cuộc tấn công, hack DeFi:

Các dự án DeFi dễ bị tấn công. Lý do có thể là vì sử dụng sai giao thức của bên thứ ba hay lỗi logic nghiệp vụ, lỗi mã hóa, cho vay nhanh, thao túng giá và các cuộc tấn công của thợ đào.

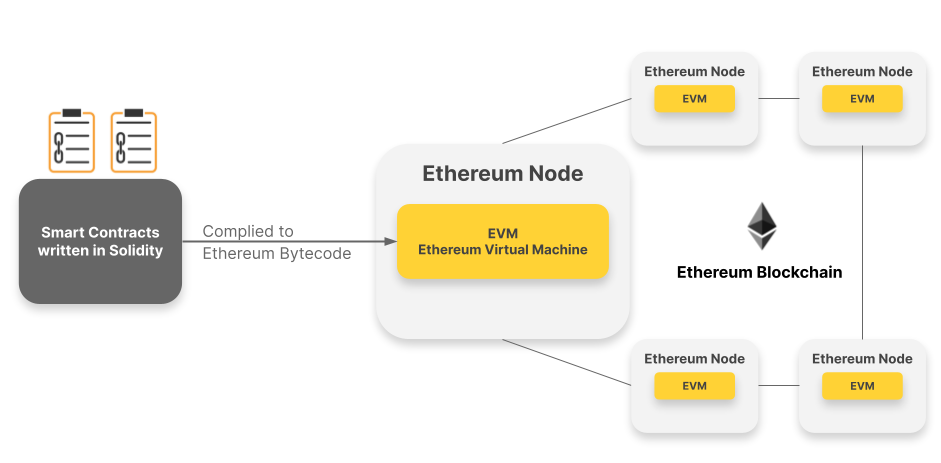
#### 2.5. Giới thiệu về Ethereum

Ethereum là nền tảng điện toán phân tán, mã nguồn mở dựa trên công nghệ chuỗi khối (Blockchain) có khả năng thực thi hợp đồng thông minh (Smart Contract).

Tức là điều khoản được ghi trong hợp đồng sẽ được thực thi một cách tự động khi các điều kiện trước đó được thỏa mãn, không ai có thể can thiệp vào. Đồng thời, Ethereum cũng cho phép các nhà phát triển xây dựng các ứng dụng phi tập trung (DApps) và các tổ chức tự trị phi tập trung (DAOs).

Trong đó:

* **Các tổ chức tự trị phi tập trung (DAOs - Decentralized Autonomous Organizations)** là một tổ chức được vận hành bởi các thành viên dựa trên một bộ quy tắc được mã hóa bằng code. Tất cả các thành viên đều có quyền biểu quyết các quyết định quan trọng của DAOs. Đổi lại, các thành viên tham gia DAOs phải có phần thưởng khi tham gia vận hành DAOs.
* **EVM (Ethereum Virtual Machine)** nói một cách đơn giản là một phần trong mạng Ethereum có nhiệm vụ xử lý việc triển khai và thực thi trên smart contract. EVM có trên tất cả các client (node) của mạng Ethereum, hướng đến mục tiêu như là một máy tính phi tập trung toàn cầu.



**Hình 3: Sơ đồ biểu diễn EVM**

#### 2.6. Giới thiệu về Smart Contract

* Smart Contract (Hợp Đồng Thông Minh) là một thuật ngữ mô tả một bộ giao thức đặc biệt có khả năng tự động thực hiện các điều khoản, các thoả thuận giữa các bên trong hợp đồng (ở trường hợp này là các hệ thống máy tính) nhờ sự hỗ trợ của công nghệ Blockchain.
* Toàn bộ hoạt động của Smart Contract được thực hiện một cách tự động và không có sự can thiệp từ bên ngoài, hay thông qua một bên thứ ba trung gian.

**2.6.1. Ưu điểm:**

- Tính minh bạch:

Những giao dịch được thực hiện bằng các hợp đồng thông minh rất minh bạch, có thể dễ dàng truy xuất được và không thể bị can thiệp hoặc đảo chiều.

Các điều khoản trong Smart Contract tương đương với một hợp đồng có pháp lý và được ghi lại dưới ngôn ngữ của lập trình (Với mạng Ethereum, ngôn ngữ lập trình sử dụng Solidity).

- Smart contract sử dụng được tất cả những điểm mạnh của công nghệ Blockchain

- Tính bảo mật:

Smart contract được mã hóa và phần phối về cho các node. Các thứ này bảo đảm nó sẽ không bị thất lạc hay sửa đổi mà không được bạn cho phép.

- Hiệu quả về kinh tế và nhanh gọn hầu hết các công đoạn đều được tư động hóa, và gần như loại bỏ bên trung gian.

- Tiêu chuẩn hóa

**2.6.2. Nhược điểm:**

- Nhân tố con người:

Vì toàn bộ phần mã được soạn thảo bởi con người và họ vẫn có thể mắc lỗi. Nếu smart contract đã được tải lên Blockchain, các nhà lập trình sẽ không thể nào thay đổi được nó. Một ví dụ nổi tiếng về nhận tố con người đó chính là sự kiện DAO. Lỗi lập trình đã bị một số tin tặc phát hiện và tận dụng, từ đó cướp đoạt đến 60 triệu tiền vốn của người dung.

- Tình trạng pháp lý chưa rõ ràng:

Hiện tại, Smart Contract vẫn chưa được quản lý bởi bất kỳ chính phủ nào cả. Vì thế cho nên vẫn tiềm ẩn khả năng xuất hiện mâu thuẫn nếu như các thể chế quản lý quyết định xây dựng bộ khung pháp lý dành cho hình thức smart contract còn khá mới mẻ này.

- Chi phí thực hiện:

Smart Contract không thể nào được lập nên mà không cần thông qua công đoạn lập trình. Do đó, điều cần thiết là phải có một chuyên gia lập trình dày dạn kinh nghiệm trong đội ngũ phát triển để hạn chế tối đa những sai sót có thể xảy ra đối với hợp đồng và bảo đảm cơ sở hạ tầng của công ty tương thích được với công nghệ Blockchain.

#### 2.7. Giới thiệu về Solidity

* Solidity là một ngôn ngữ high-level dùng cho ứng dụng vào Smart Contract. Nó là một ngôn ngữ hướng đối tượng được thiết kế dành riêng cho Ethereum Virtual Machine.
* Solidity là ngôn ngữ lập trình được xây dựng dưới sự thừa kế những đặc điểm phù hợp của các ngôn ngữ lập trình khác, đặc biệt là những đặc tính liên quan đến contract. Cũng tương tự như các ngôn ngữ lập trình khác.
* Solidity sử dụng những kiểu dữ liệu thông dụng như: kiểu số nguyên - Integer, kiểu dữ liệu 0,1 hay tương ứng với true, false - boolean, kiểu chuỗi ký tự - string literals,... Ngoài ra còn rất nhiều những kiểu dữ liệu tương thích với Solidity như kiểu mảng, toán tử, enum,... Nhìn chung, ngôn ngữ Solidity cho phép người dùng sử dụng gần như tất cả các kiểu dữ liệu phổ biến hiện nay.

=> Như vậy, với mạng Ethereum, ngôn ngữ sử dụng cho lập trình Smart

Contract sẽ là Solidity.

#### Giới thiệu về các chuẩn ERC

* ERC viết tắt của từ Ethereum Request for Comment, là một tiêu chuẩn của các Token phát triển trên nền tảng Blockchain của Ethereum.
* ERC giúp xác định hình thức của việc tạo và cấu trúc nên một Token thông qua việc lập trình Smart Contract (hợp đồng thông minh). Hiện tại có khá nhiều các chuẩn ERC như ERC20, ERC1155, ERC721, ERC948,..

Cách viết của các token này có thể là ERC20, ERC 20 hoặc ERC-20.

* Trong đề tài lần này, với mục đích và ứng dụng đã được đề ra, chúng ta sẽ sử dụng chuẩn ERC-20. ERC20 là một tiêu chuẩn kỹ thuật được sử dụng để phát hành và triển khai token trên mạng lưới Ethereum, một dạng Fungible Token.
* ERC20 cung cấp cho các nhà phát triển danh sách các quy tắc phải tuân theo cho phép các ERC20 hoạt động liền mạch trong nền tảng [Ethereum](https://coin98.net/ethereum-la-gi).
* ERC20 được đề xuất vào tháng 11 năm 2015 bởi [Vitalik Buterin](https://coin98.net/vitalik-buterin-la-ai) và Fabian Vogelsteller. Bằng cách làm theo phác thảo, các nhà phát triển không cần phải phát minh lại cấu trúc nào khác. Thay vào đó, họ có thể xây dựng trên một nền tảng đã được sử dụng trong toàn ngành.

**2.8.1. Ưu điểm:**

- Khả năng thay thế lẫn nhau (Fungible token):

Mỗi ERC20 token có thể thay thế lẫn nhau, tức là mỗi đơn vị có thể khả năng sử dụng và giá trị tương đương. Nếu bạn nắm giữ 1 USDC, việc bạn nắm giữ token cụ thể nào không quan trọng. Bạn có thể giao dịch, trao đổi nó với token của người khác và chúng vẫn giống hệt nhau về mặt chức năng.

Điều này rất có lợi, nếu token của bạn có mục tiêu trở thành một loại tiền tệ nào đó. Bạn sẽ không muốn các đơn vị riêng lẻ có các đặc điểm khác biệt, bởi điều này khiến chúng không thể thay thế được. Điều này có thể khiến một số token trở nên có giá trị hơn – hoặc ít có giá trị hơn – những token khác, làm suy yếu mục đích sử dụng của chúng.

- Tính linh hoạt:

Các ERC20 token có khả năng tùy chỉnh cao và có thể được điều chỉnh cho phù hợp với nhiều ứng dụng khác nhau.

Ví dụ: ERC20 Token có thể được sử dụng như là tiền và giao dịch trong các [AMM](https://coin98.net/amm), hoặc đem đi gửi để lấy lãi suất trong các nền tảng [Lending](https://coin98.net/lending-la-gi),...

- Sự phổ biến:

Sự phổ biến của ERC20 trong không gian [Crypto](https://coin98.net/cryptocurrency-la-gi)là một lý do rất thuyết phục để sử dụng nó làm một tiêu chuẩn chung. Có rất nhiều sàn giao dịch, ví và hợp đồng thông minh đã tương thích với ERC20 token. Hơn nữa, sự hỗ trợ của các nhà phát triển và tài liệu cũng rất phong phú.

**2.8.2 Nhược điểm:**

**-** Khả năng mở rộng:

Nhiều mạng [blockchain](https://coin98.net/blockchain-101)khác, khả năng mở rộng là thách thức lớn đối với Ethereum. Hiện tại, việc mở rộng quy mô của Ethereum diễn ra không tốt, việc cố gắng gửi một giao dịch vào thời gian cao điểm dễ dẫn đến phí cao và sự chậm trễ. Điều này ảnh hưởng khả năng sử dụng của ERC20 token.

- Rủi ro lừa đảo:

Mặc dù đây không phải là lỗi của công nghệ, nhưng việc dễ dàng ra mắt token mới có thể coi là một nhược điểm của ERC20 ở một số khía cạnh. Hiện tại rất dễ để tạo ra một ERC20 token đơn giản, có nghĩa là bất kỳ ai cũng có thể làm điều đó, dù với mục đích tốt hay xấu.

#### Giới thiệu về IDO và cách hoạt động của IDO

- **IDO** là từ viết tắt của của Initial Decentralized Exchange Offering. Đây cũng là một hình thức gọi vốn, nhưng nơi gọi vốn không phải là sàn tập trung (Centralized Exchange) như Binance, mà là các nền tảng phi tập trung

- **IDO** là một hình thức phát hành token trên sàn giao dịch phi tập trung (DEX). Bể thanh khoản (Liquidity Pool) đóng một vai trò thiết yếu trong IDO, vì chúng giúp tạo ra thanh khoản cho token sau khi mở bán. Một IDO điển hình cho phép người dùng khóa tiền để đổi lấy các token mới trong sự kiện tạo token. Sau đó, một phần nguồn vốn đã huy động cùng với token được thêm vào Liquidity Pool, trước khi được trả lại cho dự án sau đó.

- **IDO** là một cách phân phối token đơn giản và tiết kiệm chi phí. Các IDO đã xuất hiện được một thời gian, nhưng hình thức này vẫn đang phát triển và tạo ra các mô hình mới như phát hành qua [Farm lần đầu (IFO)](https://coin68.com/ifo-intial-farm-ofering/#:~:text=IFO%20l%C3%A0%20m%E1%BB%99t%20lo%E1%BA%A1i%20ho%E1%BA%A1t,b%E1%BA%B1ng%20s%E1%BB%91%20LP%20token%20n%C3%A0y.). Yêu cầu KYC (Know Your Customer, xác minh danh tính ) ngày càng tăng khi lĩnh vực này dần đi vào khuôn khổ.

**2.9.1. Cách hoạt động của IDO:**

Các quy tắc và giai đoạn của IDO phụ thuộc vào DEX thực thi, nhưng có một số phương pháp phổ biến:

a) Sau quá trình kiểm duyệt, một dự án được chấp nhận để IDO trên DEX. Dự án cung cấp token với một mức giá cố định và người dùng khóa tiền của họ để đổi lại những token này. Các nhà đầu tư sẽ nhận được token trong sự kiện tạo token (TGE) sau đó.

\*\* TGE được viết tắt từ “Token Generation Event”. Đó là một sự kiện tạo token như một hoạt động huy động vốn cho Dự án bằng cách phát hành token dưới nhiều hình thức bán công khai và bán riêng lẻ hoặc cung cấp các Token ban đầu.

Sự kiện này thường được sử dụng như một công cụ để thu hút sự công khai và tham gia vào các cộng đồng tiền điện tử với mục tiêu huy động động vốn (gây Quỹ).

b) Thông thường, có một danh sách trắng (whitelist) nhà đầu tư. Bạn có thể phải hoàn thành các nhiệm vụ tiếp thị để có mặt trong danh sách hoặc chỉ cần cung cấp địa chỉ ví của mình.

1. Một phần số tiền được huy động sẽ được sử dụng để tạo ra một [bể thanh khoản](https://academy.binance.com/vi/articles/what-are-liquidity-pools-in-defi) cho token của dự án.

Phần còn lại của số vốn sẽ được trao cho đội ngũ phát triển. Sau đó, các nhà đầu tư có thể giao dịch token sau TGE (sự kiện tạo token). Thông thường, thanh khoản được cung cấp sẽ bị khóa trong một khoảng thời gian nhất định.

1. Tại sự kiện TGE, các token được chuyển cho người dùng và bể thanh khoản được mở để giao dịch.

**2.9.2. Ưu điểm:**

Theo thời gian, việc phát hành token đã dần trở nên công bằng và an toàn hơn với các nhà đầu tư. Trong đó, IDO có một số lợi thế khác biệt:

- Bạn không cần phải giao dịch trực tiếp với một dự án và tin tưởng vào các hợp đồng thông minh của họ:

Một nền tảng IDO đáng tin cậy sẽ có các lần mở bán token thành công. Nếu các hợp đồng thông minh này là hoàn toàn giống nhau, bạn có thể tin tưởng vào việc mở bán token.

- Thanh khoản ngay lập tức sau khi mở bán:

Các IDO sẽ khóa một số tiền huy động được trong các bể thanh khoản để tạo ra một thị trường thanh khoản ngay sau khi mở bán. Điều này giúp giảm độ [trượt](https://academy.binance.com/vi/articles/bid-ask-spread-and-slippage-explained) và [biến động giá](https://academy.binance.com/en/glossary/volatility).

- Không cần đăng ký:

Bạn chỉ cần có ví và tiền mã hóa để tham gia đợt mở bán và không bắt buộc phải cung cấp thông tin cá nhân. Điều này làm cho quá trình này mở với tất cả đối tượng người dùng. Tuy nhiên, việc thiếu các quy trình KYC hoặc AML có thể xem là một điểm bất lợi (đọc thêm về điều này bên dưới).

- IDO có giá cả phải chăng và giúp nhà đầu tư dễ tiếp cận các dự án:

Việc phát hành token thông qua DEX thường dễ dàng và rẻ hơn đối với một dự án nhỏ, ít nổi tiếng; hơn là qua một sàn giao dịch lớn, tập trung.

- IDO thường có các biện pháp chống cá voi, có nghĩa là không một nhà đầu tư duy nhất nào có thể mua được một số lượng lớn các token.

**2.9.3. Nhược điểm:**

Một số điểm mạnh của IDO cũng là điểm yếu của nó. Những vấn đề này chủ yếu xuất phát từ các khía cạnh phi tập trung và ẩn danh của IDO.

- Không có quá trình KYC hoặc AML:

Thông thường, các nhà đầu tư và dự án sẽ được bảo vệ khi hoàn thành các bước kiểm tra thích hợp. Các biện pháp này giúp phòng tránh việc rửa tiền bất hợp pháp và trốn tránh các lệnh trừng phạt kinh tế.

Ví dụ: việc tham gia IDO ở một số quốc gia nhất định có thể là bất hợp pháp nếu token được coi là chứng khoán.

- Có ít sự [thẩm định](https://academy.binance.com/vi/articles/12-terms-every-crypto-trader-should-know) với các dự án :

Việc phân phối token thông qua IDO khá dễ dàng. Vì vậy, so với IEO - phát hành thông qua một sàn giao dịch lớn được quản lý, IDO có nhiều dự án không đáng tin cậy hơn.

**2.9.4. Sự khác biệt giữa IDO, IEO, ICO**



**Hình 4: Sự khác biệt giữa IDO, IEO, ICO**

#### Giới thiệu về Liquidity Pool

**2.10.1. Khái niệm Liquidity (thanh khoản)**

Liquidity hay còn gọi là tính thanh khoản, thể hiện qua việc mua, bán một khối lượng lớn tiền điện tử mà không (hoặc rất ít) gây tác động đến giá của đồng tiền điện tử đó.

Thanh khoản không chỉ được dùng trong thị trường Crypto, mà còn ở chứng khoán, hay ở bất cứ tài sản giao dịch nào. Một tài sản được xem là thanh khoản cao khi có thể bán được một cách nhanh chóng mà giá không giảm đáng kể so với dự định, có thể ví dụ như BTC, ETH,…



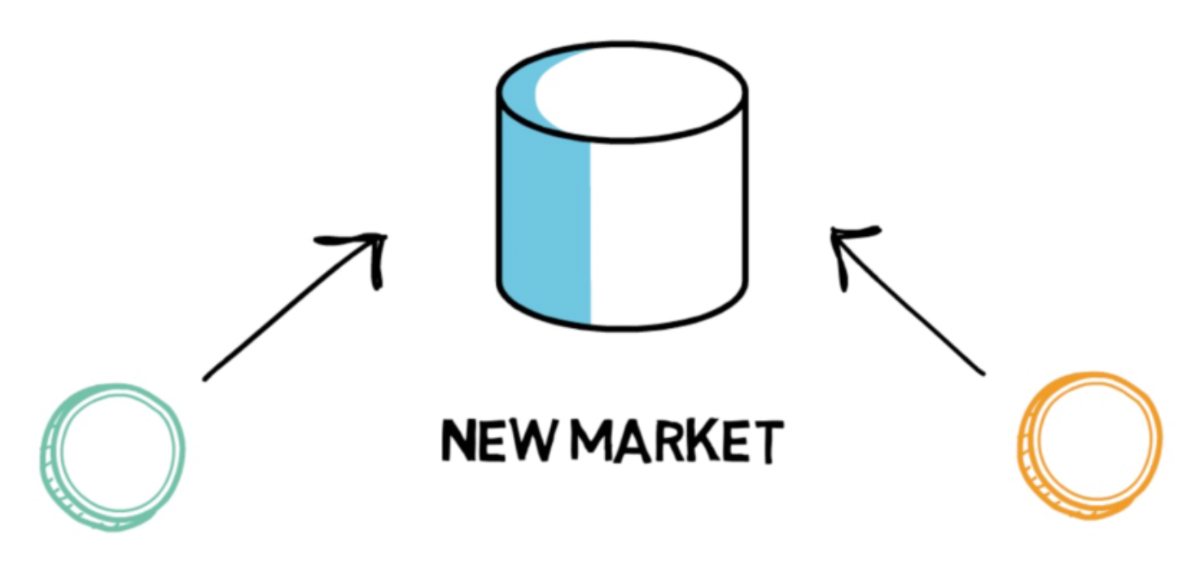
**Hình 5: Sơ đồ biểu diễn thanh khoản**

**2.10.2.** **Liquidity pool (bể thanh khoản)**

Liguidity pool là một nhóm coin hoặc token được khoá (lock) trong một [hợp đồng thông minh](https://coin98.net/smart-contract-la-gi). Chúng tạo điều kiện cho phép các tài sản kỹ thuật số được di chuyển theo cách tự động và không cần sự cho phép (permissionless) thông qua việc sử dụng các nhóm thanh khoản.

**2.10.3. Cách hoạt động:**

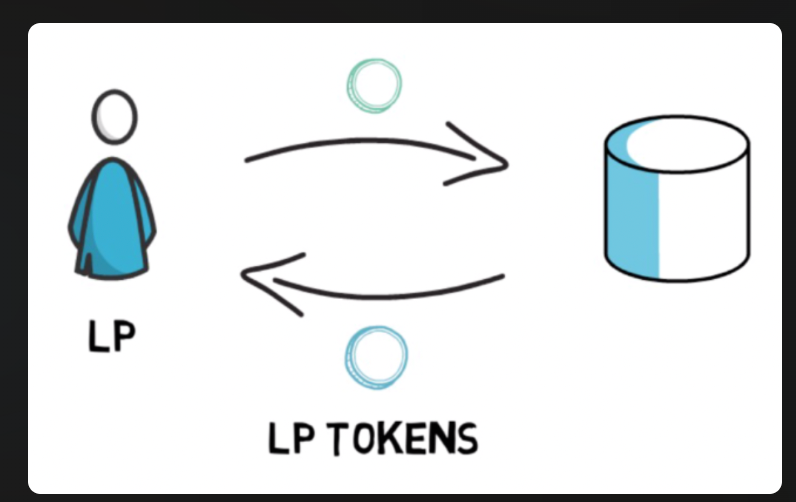
Một trong những nhóm người quan trọng nhất đề Liquidity Pool hoạt động hiệu quả là những người cung cấp thanh khoản cho Liquidity Pool đó, hay còn gọi là Liquidity Provider.



**Hình 6: Sơ đồ biểu diễn pool**

Vì vậy Liquidity Pool trong tiền điện tử nếu muốn hoạt động hiệu quả thì chúng cần được thiết kế kèm theo các khuyến khích (incentive) thích hợp để các Liquidity Provider cung cấp tài sản của họ vào Liquidity Pool.

Khi người dùng cung cấp tính thanh khoản vào pool, nhà cung cấp thanh khoản thường được nhận lại Liquidity Pool token. LP token đại diện cho cổ phần tài sản của họ trong pool chung và chúng cũng có thể được sử dụng trong toàn bộ hệ sinh thái DeFi với nhiều khả năng khác nhau.



**Hình 7: Sơ đồ biểu diễn mối liên hệ liquidity provider và pool**

#### Giới thiệu về Launchpad và cách thức hoạt động

Launchpad là nơi các dự án hiện nay sử dụng để phát hành token và gọi vốn IDO, có thể kể đến một vài cái tên như Polkastarter, DAO Maker, Solstarter, BSCPad,…

Là một nền tảng bệ phóng tiền điện tử, hay còn được gọi là vườn ươm tiền điện tử, một nền tảng cho phép các dự án blockchain huy động vốn bằng cách bán trước token cho các nhà đầu tư trước khi token được bán công khai.

Thông thường, nền tảng này sẽ được vận hành bởi một sàn giao dịch tiền mã hóa hoặc một nền tảng riêng tùy vào tầm nhìn của các dự án khác nhau.

Thông qua Launchpad, nhà đầu tư có cơ hội đầu tư vào những dự án hấp dẫn ngay từ rất sớm, mà trước đây chỉ có những nhà đầu tư tổ chức mới có cơ hội đầu tư. Còn đối với các công ty Startup thì huy động vốn thông qua Launchpad có mức phí tương đối thấp, phù hợp với những Startup eo hẹp về vốn đầu tư ban đầu.

Đầu tư thông qua Launchpad đang trở nên rất phổ biến ngày nay và sẽ tiếp tục phát triển trong vài năm tới.

**2.11.1. Cách hoạt động**

Để hiểu rõ cách thức hoạt động của Launchpad, bạn cần hiểu cách các dự án mới huy động vốn cho họ bằng cách nào.

- Bước 1: Nhóm phát triển dự án mới sẽ tung ra một sản phẩm/dịch vụ mà họ đang phát triển.

- Bước 2: Họ tiếp tục cho ra mắt đồng token riêng của mình. Đây được xem là thành phần không thể thiếu đối với chiến lược phát triển của các dự án.

- Bước 3: Nhóm phát triển sẽ bán những đồng token cho các nhà đầu tư ban đầu để huy động vốn với mức giá thường được định giá thấp hơn khi bán công khai.

- Bước 4: Token được lưu hành công khai trên thị trường.

- Bước 5: Khi dự án phát triển, giá trị của những đồng token tăng. Nhờ đó, các nhà đầu tư ban đầu – những người tham gia dự án sớm nhất và được mua token với giá rẻ sẽ được hưởng nhiều lợi nhuận hơn và đây chính là phương thức vận hành của Launchpad trong crypto.

**2.11.2. Ưu điểm**

* Giúp các nhà đầu tư tiếp cận sớm dự án mới trước khi được phát hành trên thị trường.
* Mua token với mức giá thấp hơn giá khi token được phát hành.
* Cơ hội nhận một nguồn lợi nhuận khi token được niêm yết.

**2.11.3. Nhược điểm**

* Giống như việc đầu tư vào tiền điện tử, việc đầu tư vào Launchpad cũng mang lại một số rủi ro nhất định.
* Phải có kiến thức về tiền điện tử, DeFi và các mạng Blockchain để có thể lựa chọn dự án phù hợp.

#### Giới thiệu về framework web3

- Web3.js là một thư viện JavaScript mã nguồn mở (GNU Lesser General Public License phiên bản 3) được xây dựng bởi Ethereum Foundation, bao gồm các chức năng giao tiếp với các node Ethereum thông qua giao thức JavaScript Object Notation

- Remote Procedure Call (JSON-RPC) . Nói cách khác, nó là một thư viện JavaScript hỗ trợ các nhà phát triển tương tác với chuỗi khối Ethereum.

- Web3.js có một lớp chính được gọi là web3. Hầu hết các chức năng của thư viện có thể được tìm thấy trong danh mục này.

* 5 mô-đun khác tạo nên web3js là:
  + - web3-eth
    - web3-shh
    - web3-bzz
    - web3-net
    - web3-utils

**2.12.1. Web3-eth**

- Mô-đun web3-eth chứa các chức năng cho phép người dùng web3.js tương tác với chuỗi khối Ethereum. Cụ thể, các chức năng này có thể tương tác với các hợp đồng thông minh, tài khoản thuộc sở hữu bên ngoài, các node, khối được khai thác và các giao dịch.

Dưới đây là ba ví dụ minh họa:

- Chức năng của \_web3.eth.getBalance\_ là lấy số dư Ethereum của một địa chỉ trong một khối cụ thể

- Vai trò của \_web3.eth.signTransaction\_ là ký giao dịch

- Chức năng của \_web3.eth.sendSignedTransaction\_ là gửi giao dịch đã ký đến chuỗi khối Ethereum.

**2.12.2. Web3-shh**

- Chức năng của mô-đun web3-shh là cho phép bạn tương tác với giao thức Whisper. Whisper là một giao thức truyền thông điệp, mục đích của nó là truyền thông điệp dễ dàng và truyền thông không đồng bộ mức thấp.

Dưới đây là hai ví dụ minh họa:

* \_web3.shh.post\_post gửi tin nhắn Whisper cho web
* \_web3.shh.subscribe\_Tạo đăng ký tin nhắn Whisper đến

**2.12.3. Web3-bzz**

- Chức năng của mô-đun web3-bzz là cho phép bạn tương tác với Swarm. Nó là một nền tảng lưu trữ phi tập trung và dịch vụ phân phối nội dung có thể được sử dụng để lưu trữ các tệp như hình ảnh hoặc video cho các ứng dụng phi tập trung.

Dưới đây là hai ví dụ minh họa:

- Chức năng của \_web3.bzz.upload\_: cho phép tải các tệp và thư mục lên Swarm

- Vai trò của \_Web3.bzz.download\_ là cho phép bạn tải xuống các tệp và thư mục từ Swarm

**2.12.4. Web3-net**

Chức năng của mô-đun web3-net là cho phép bạn tương tác với các thuộc tính mạng của các node Ethereum. Thông qua web3-net, bạn có thể sử dụng giao thức được liên kết với thông tin bạn cần lấy, sau đó là .net (được chỉ định bằng \* ở đây, có nghĩa là chọn web.eth.net, web3.shh.net hoặc web3.bzz.net) để tìm kiếm Thông tin về node này.

Dưới đây là hai ví dụ minh họa:

* web3. \*. net.getID trả về ID mạng
* web3. \*. net.getPeerCount trả về số lượng đồng nghiệp được kết nối với node

**2.12.5. Web3-utils**

- Mô-đun web3-utils cung cấp cho bạn các chức năng tiện ích, có thể được sử dụng trong các ứng dụng phi tập trung Ethereum và các mô-đun web3.js khác. Các chức năng tiện ích có thể được sử dụng lại, giúp việc viết mã dễ dàng hơn và rất phổ biến trong JavaScript và các ngôn ngữ lập trình khác. Web3-utils chứa các hàm tiện ích để chuyển đổi số, xác minh xem các giá trị có đáp ứng các điều kiện nhất định hay không và tìm kiếm tập dữ liệu.

Dưới đây là ba ví dụ minh họa:

* \_web3.utils.toWei\_ chuyển đổi ether sang Wei
* \_web3.utils.hexToNumberString\_ chuyển đổi một giá trị thập lục

phân thành một chuỗi

* web3.utils.isAddress, để xác minh xem một chuỗi cụ thể có phải

là địa chỉ Ethereum hợp lệ hay không.

## Chương 3

## XÂY DỰNG HỆ THỐNG LAUNCHPAD IDO

## TRÊN NỀN TẢNG EVM

### 3.1. Tổng quan về ứng dụng

Tổng quan: Với đề tài xây dựng hệ thống launchpad IDO trên nền tảng EVM, ứng dụng sẽ được xây dựng trên nền tảng phi tập trung. Từ đó cho phép IDO các token. Nó được xem như là sự gọi vốn. Các đợt gọi vốn diễn ra như một sự kiện mở bán token với giá rẻ. Với launchpad, các nhà đầu tư cũng có thể mua các token sớm, trước khi sự kiện mở bán được diễn ra chính thức.

### 3.2. Các phần chính của ứng dụng:

* Mạng Blockchain riêng tư để đảm bảo tính bảo mật của dữ liệu. Ganache để dựng một mạng Blockchain private để lưu trữ dữ liệu
* Xây dựng các Smart Contracts theo yêu cầu đề tài được đặt ra
* Lập trình Web3js
* Xây dựng giao diện hỗ trợ tương tác giữa người dùng và mạng Blockchain

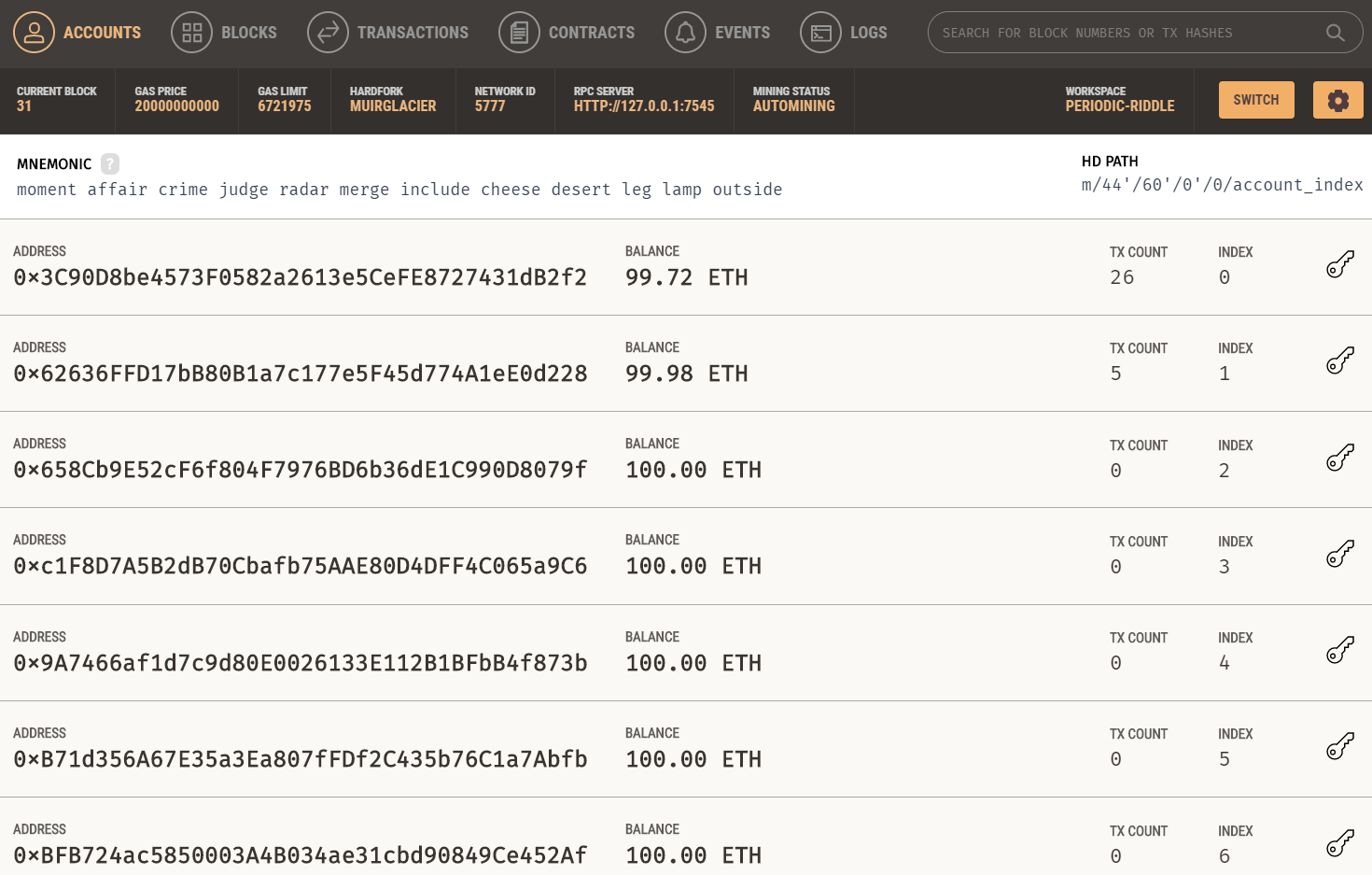
### 3.3. Xây dựng mạng Blockchain

* Trong đề tài này, em sẽ sử dụng **Ganache** để dựng một mạng Blockchain private để lưu trữ các Smart Contracts cũng như theo các thông tin, cấu trúc đã đề ra.

- Sử dụng **Truffle** để deploy và **Hardhat** để verify

**\*\* Truffle**: Đây là một framework để phát triển Ethereum Smart Contract : https://github.com/trufflesuite/truffle . Nó giúp xây dựng cấu trúc và một số lệnh để viết SC

**\*\* Hardhat:** là một môi trường mà các nhà phát triển sử dụng để kiểm tra, biên dịch, triển khai và gỡ lỗi các dApp dựa trên chuỗi khối Ethereum.



**Hình 8: Giao diện Ganache**

### 3.4. Lập trình Smart Contract

Sử dụng ngôn ngữ Solidity cho phần code và IDE Remix Ethereum cho phần deploy

**3.4.1. Contract: PoolModifier.sol**

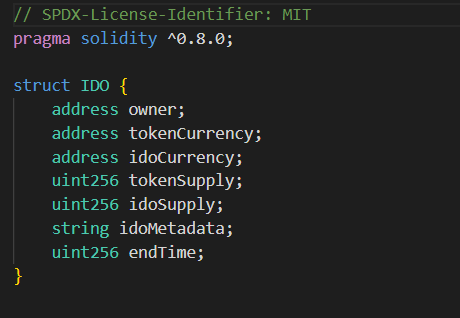
Kiểm tra các điều kiện trước khi các đoạn mã code trong phương thức đó được thực thi (điều này là vô cùng quan trọng trong việc đảm bảo được tính an toàn trong Smart Contract).



**Hình 9: PoolModifier.sol**

**3.4.2. Contract: IDO.sol**

Cấu trúc Struct cho phép tạo các kiểu dữ liệu phức tạp hơn có nhiều thuộc tính.

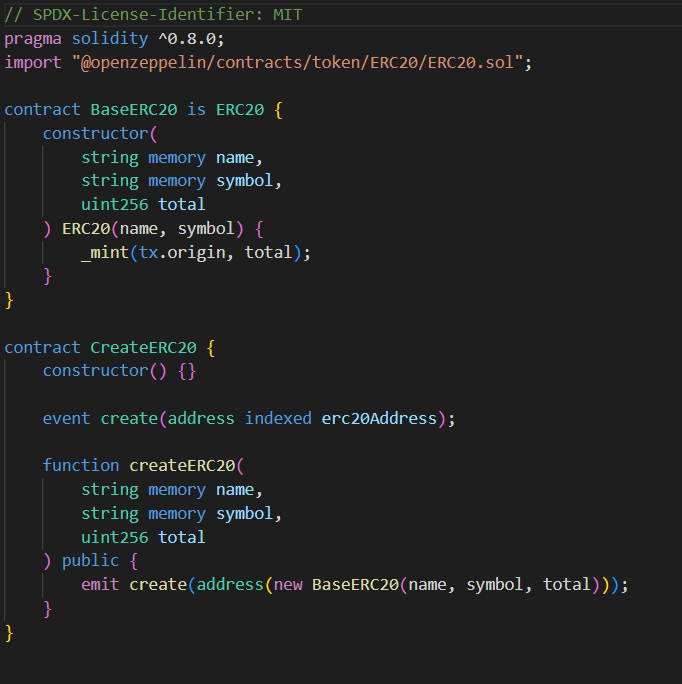


**Hình 10: Contract IDO.sol**

**3.4.3. Contract: CreateERC20.sol**

- Sử dụng chuẩn ERC20

- Mint các token được yêu cầu cho dự án



**Hình 11: CreateERC20.sol**

**3.4.4. Contract: Pool.sol**

Bao gồm các function:

- addIDO: Tạo IDO

- buyIDO: Mua token từ đợt IDO

- claimLeftIdo: Lấy số token dư thừa của đợt IDO sau khi hết hạn

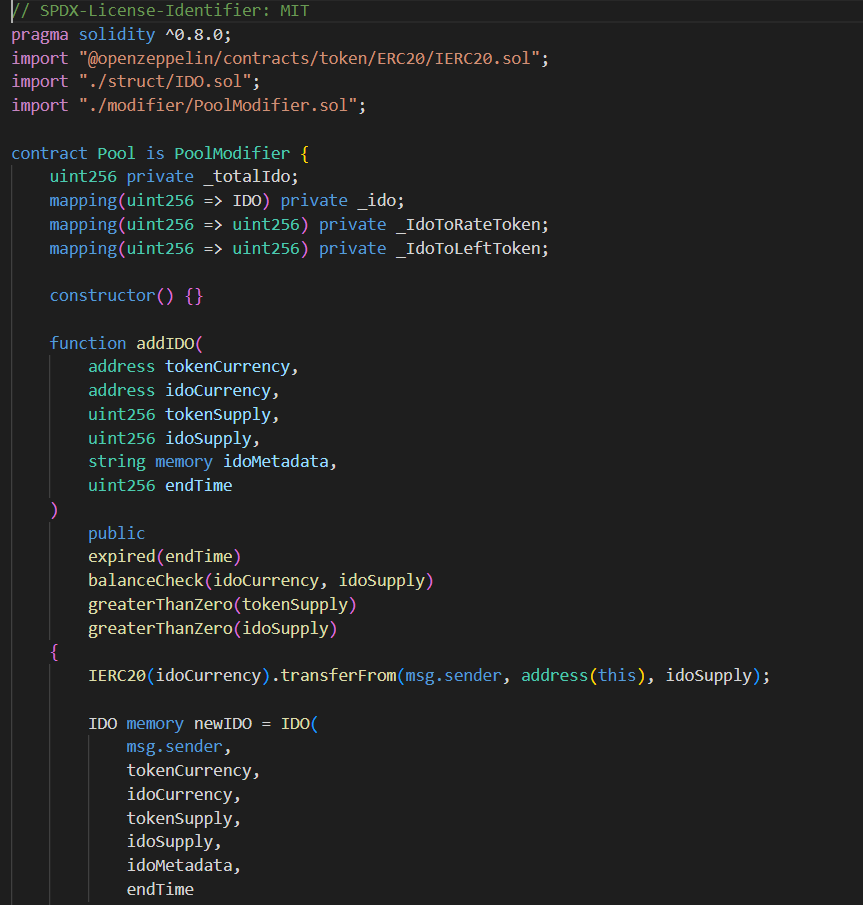
- calculateRateIdo: Tính toán tỷ lệ cho IDO

- isIDOEnded: IDO đã hết hạn hay chưa (True or False)

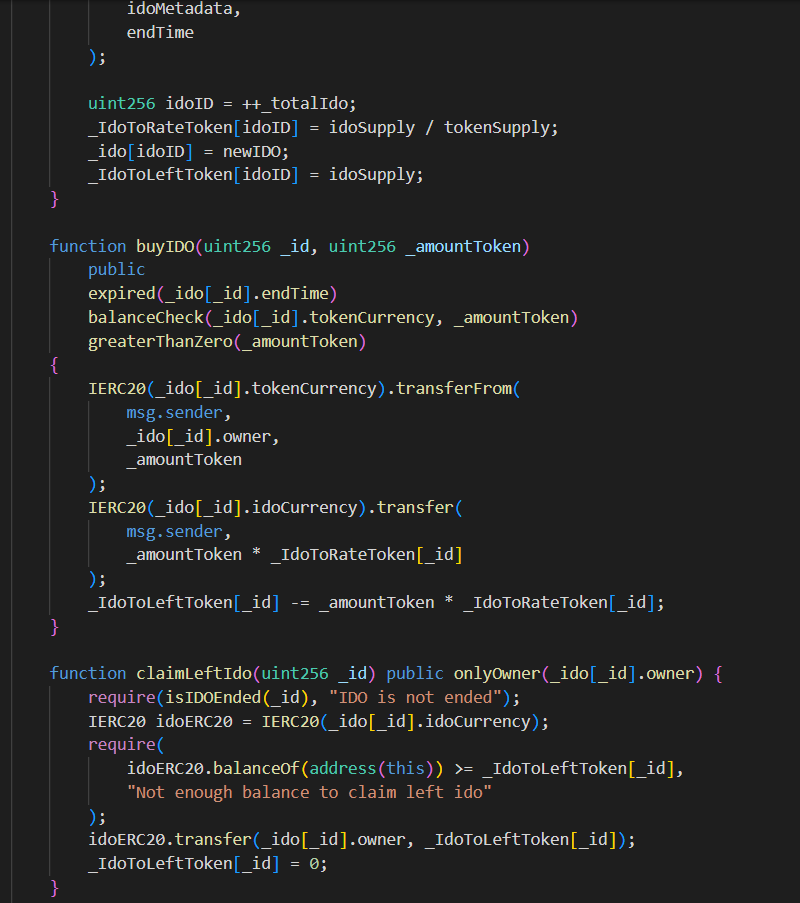
- getIDO: Thông tin IDO

- getLeftIDO: Xem còn lại bao nhiêu token của đợt IDO

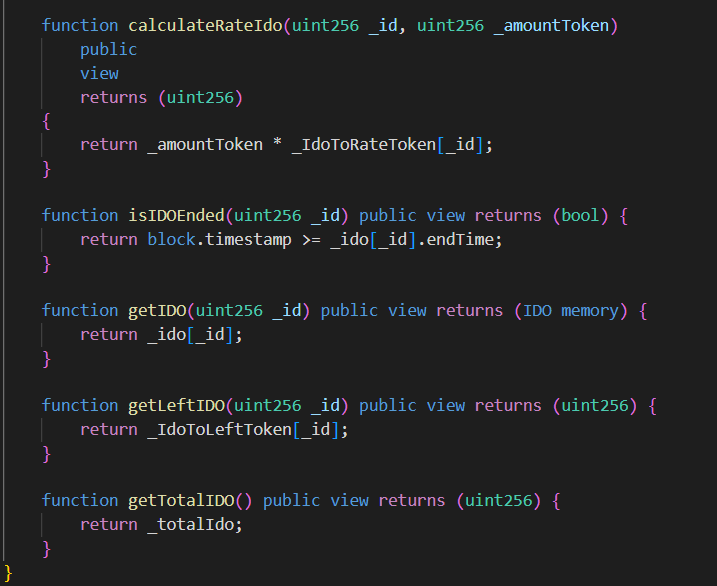
- getTotalIDO: id của đợt IDO (bắt đầu từ 1)



**Hình 12: Contract Pool.sol**



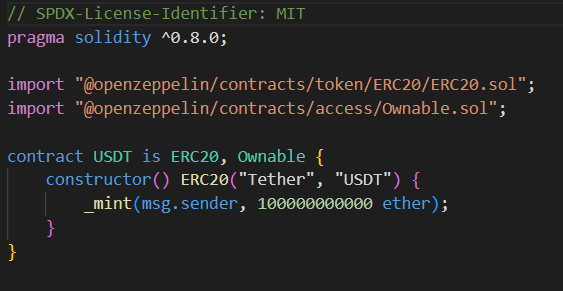
**Hình 13: Contract Pool.sol**



**Hình 14: Contract Pool.sol**

**3.4.5 Contract: USDT.sol**

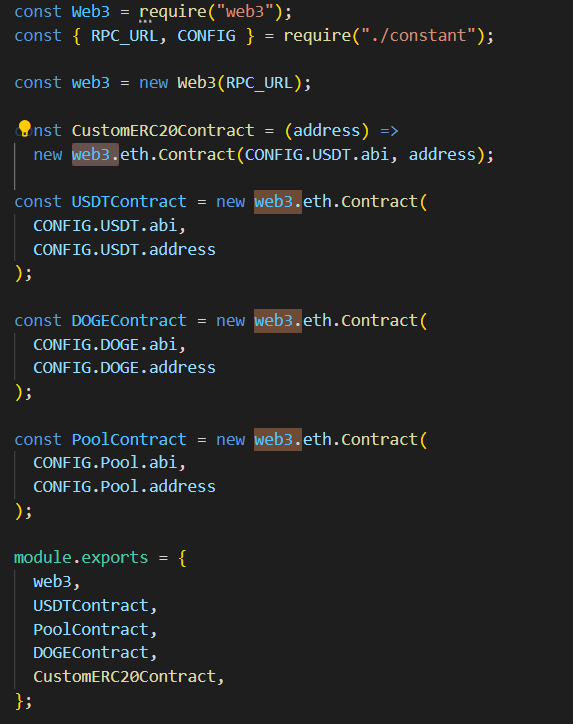
Sử dụng ERC20 để mint USDT



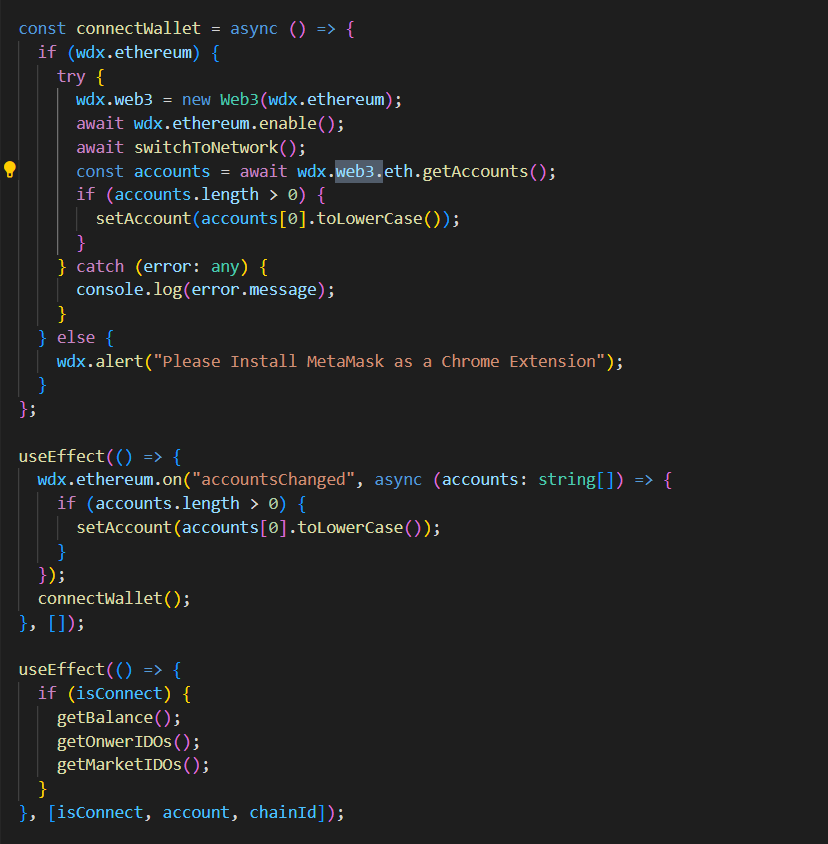
**Hình 15: Contract USDT.sol**

### 3.5: Lập trình Web3js

- Sử dụng web3js để tương tác giữa front-end và blockchain



**Hình 16: Connect contract thông qua web3**



**Hình 17: ConnectWallet sử dụng web3**

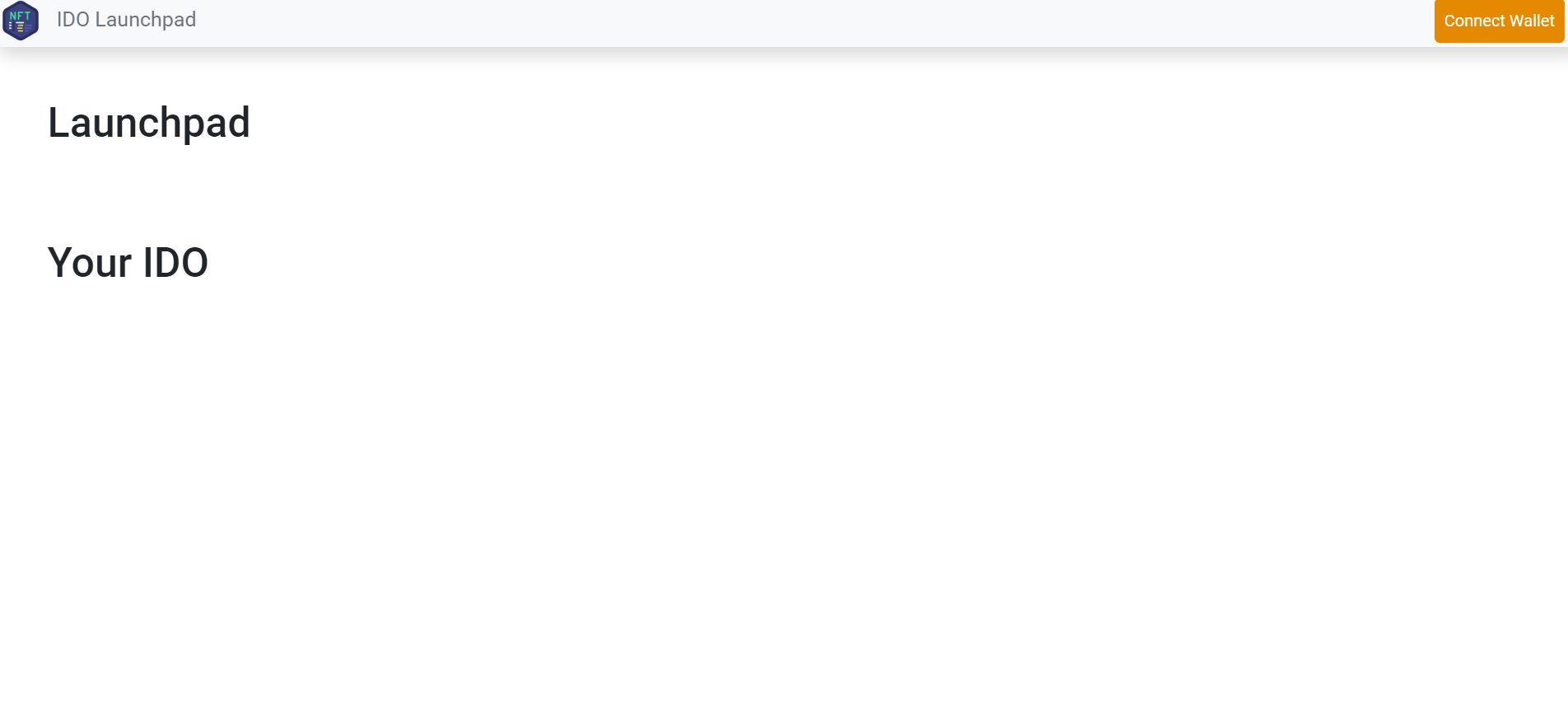


**Hình 18: Hiển thị balance hiện có của token thông qua web3**

### 3.6. Lập trình giao diện

* + 1. **Connect Wallet**

Cụ thể sẽ connect với wallet: metamask

****

**Hình 19: Giao diện trước khi connect wallet**

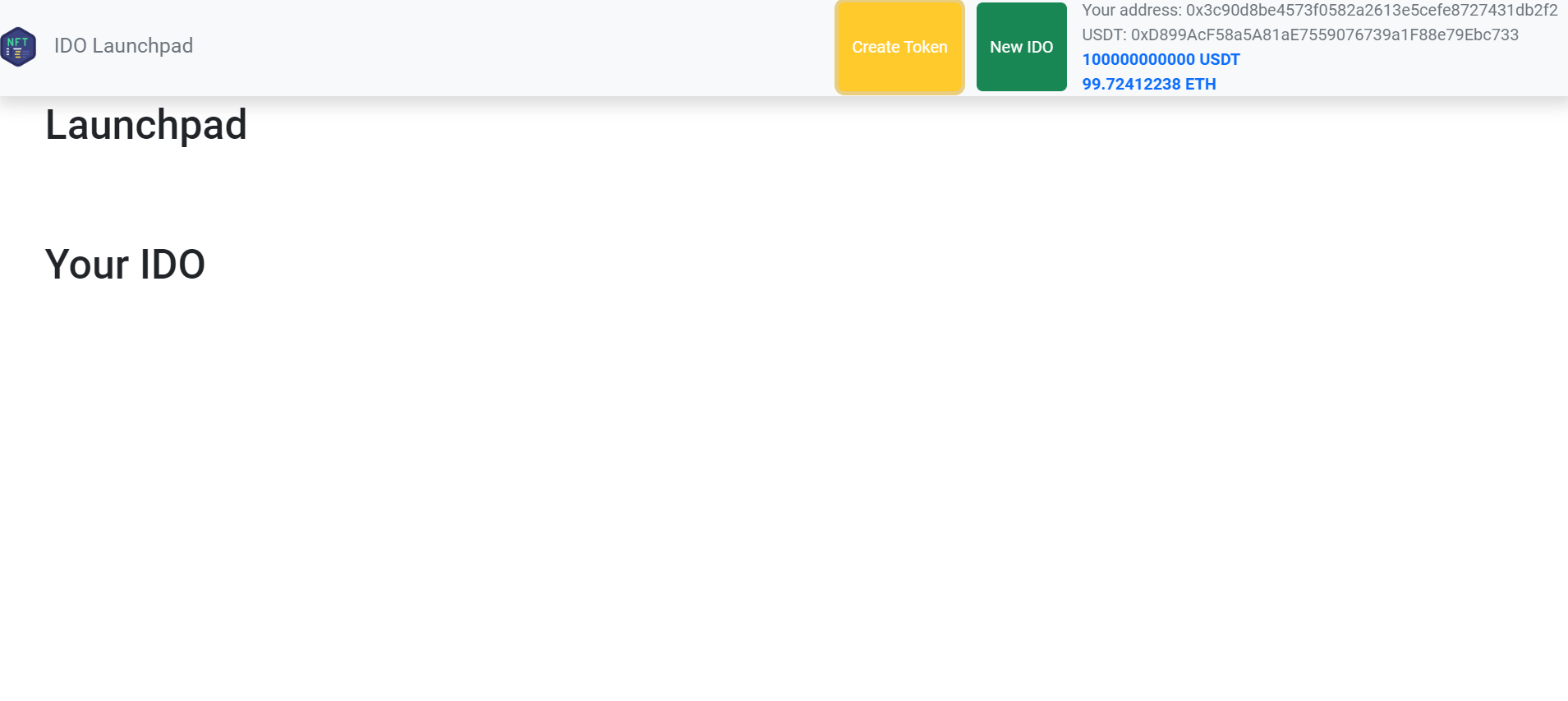
* + 1. **Giao diện sau khi connect wallet**

Sau khi connect wallet các thông tin sau sẽ được cập nhật:

- Your address: địa chỉ account deploy contract

- USDT address: địa chỉ contract sau khi mint USDT  
 - Số lượng USDT đã mint

- Số lượng ETH có trong account wallet



**Hình 20: Giao diện sau khi connect wallet**

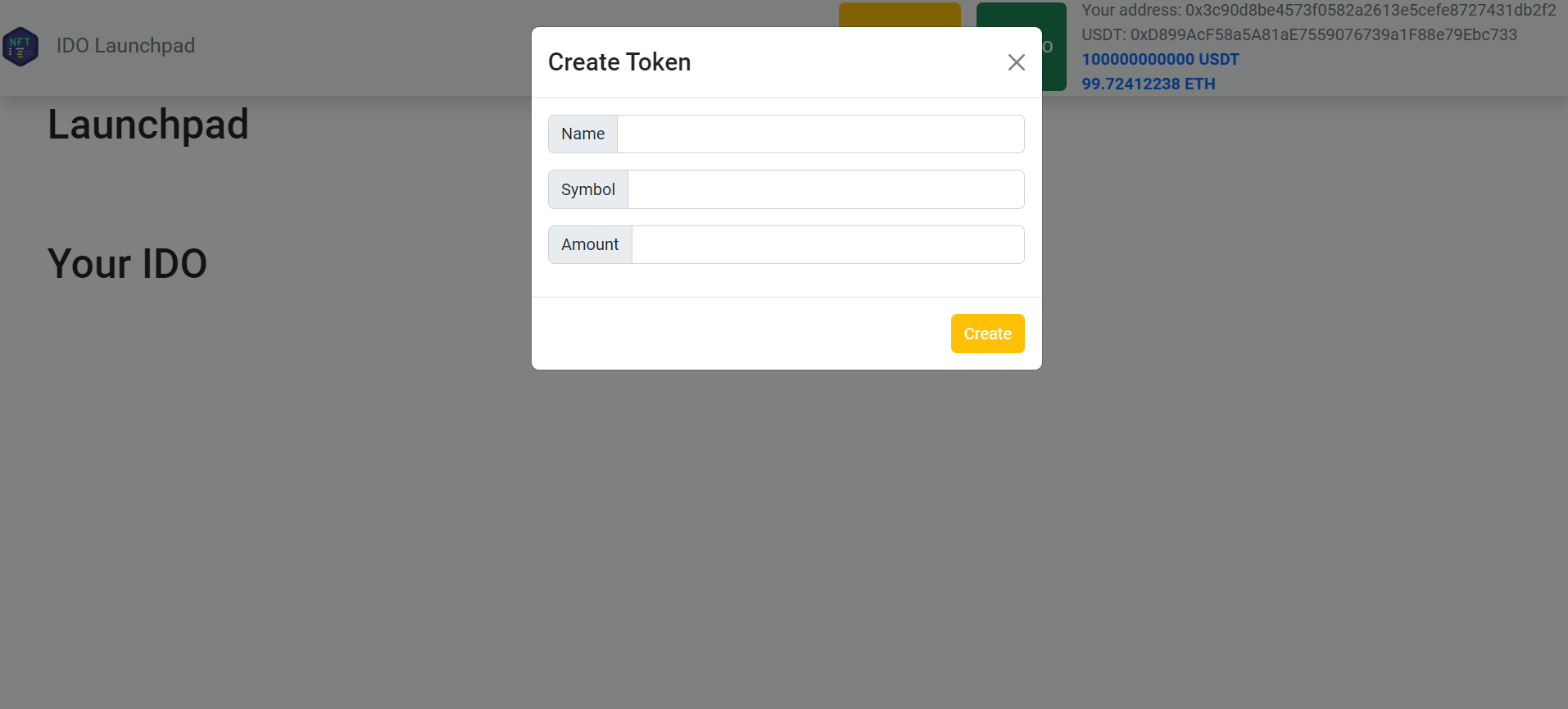
* + 1. **Giao diện Create token**

- Create name token

- Create symbol token

- Create amount token

Thực hiện mint token theo yêu cầu. Sử dụng chuẩn token ERC20 để mint



**Hình 21: Giao diện tạo token**

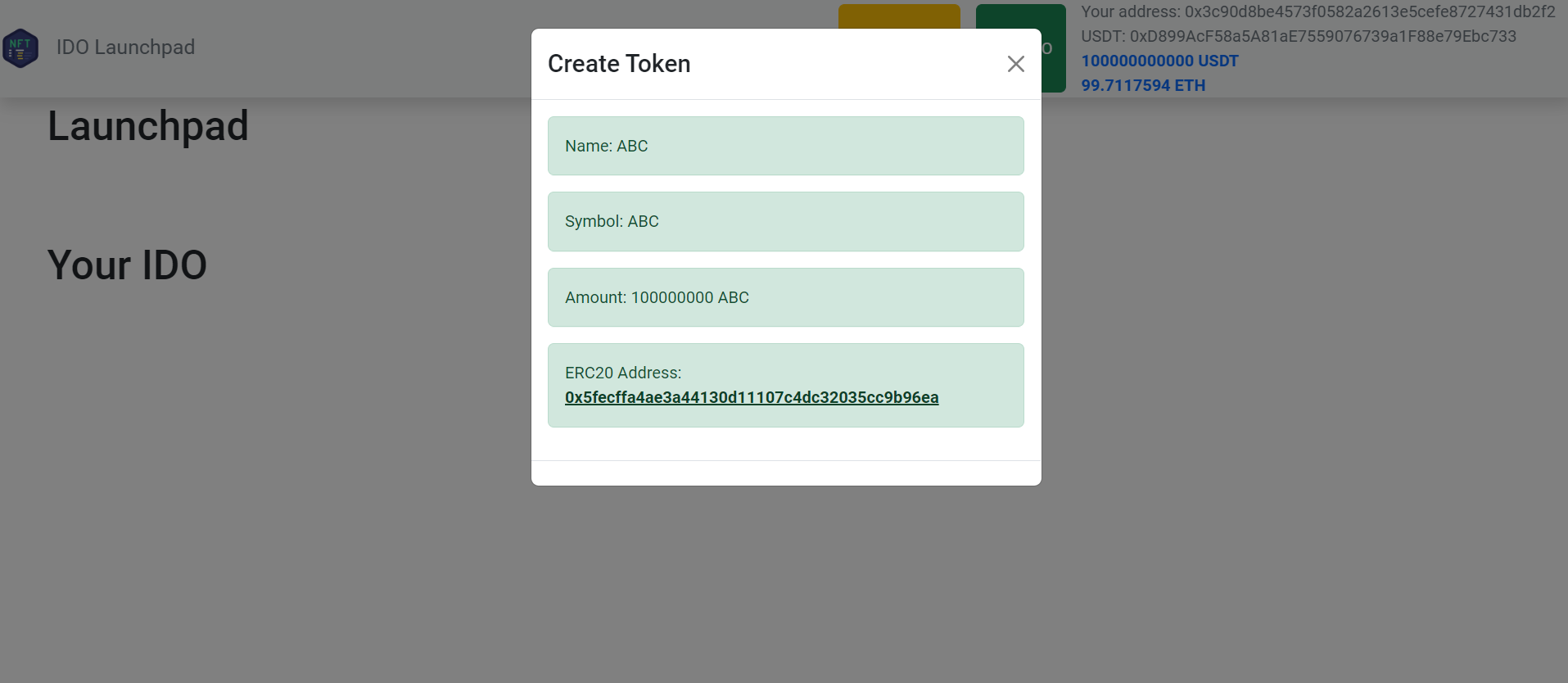
* + 1. **Sau khi create token thành công**

Các thông tin giao diện bao gồm:

- Các thông tin của token sau khi mint sẽ được hiển thị

- Hiển thị thêm address của token sau khi mint thành công

- Có thể dùng address này để import token vừa mint vào wallet



**Hình 22: Giao diện sau khi tạo token thành công**

* + 1. **Giao diện New IDO**

Thực hiện tạo các đợt IDO sau khi đã mint token muốn mở bán.

Các thông tin giao diện bao gồm:

- Thêm title

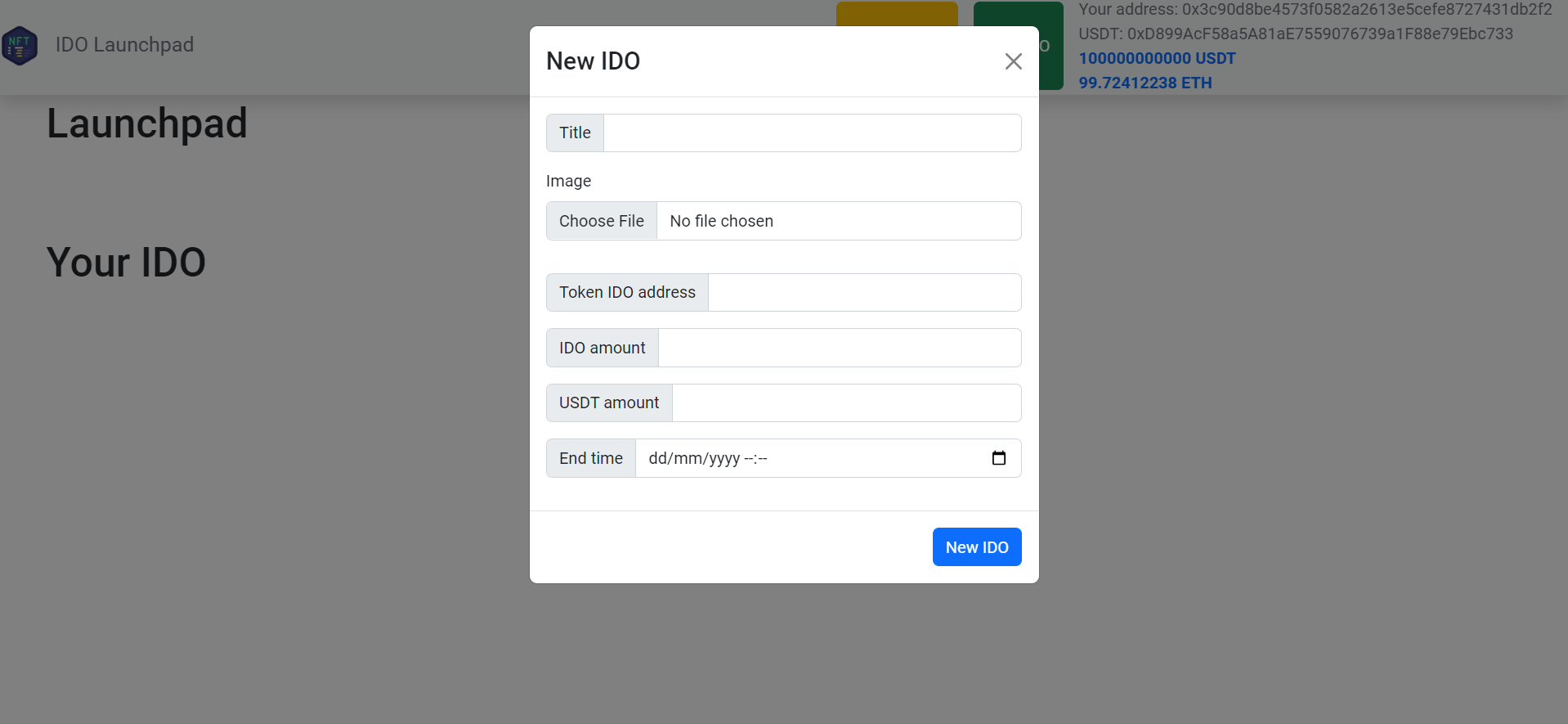
- Chọn ảnh đại diện cho đợt IDO

- Address của token IDO

- Số lượng token IDO

- Số lượng USDT

- Thời gian hết hạn của đợt IDO



**Hình 23: Giao diện khởi tạo IDO**

* + 1. **Giao diện sau khi khởi tạo đợt IDO:**

Sau khi khởi tạo đợt IDO thành công, các nhà đầu tư nếu có token USDT thì đều có thể tham gia mua token IDO

Các thông tin giao diện bao gồm:

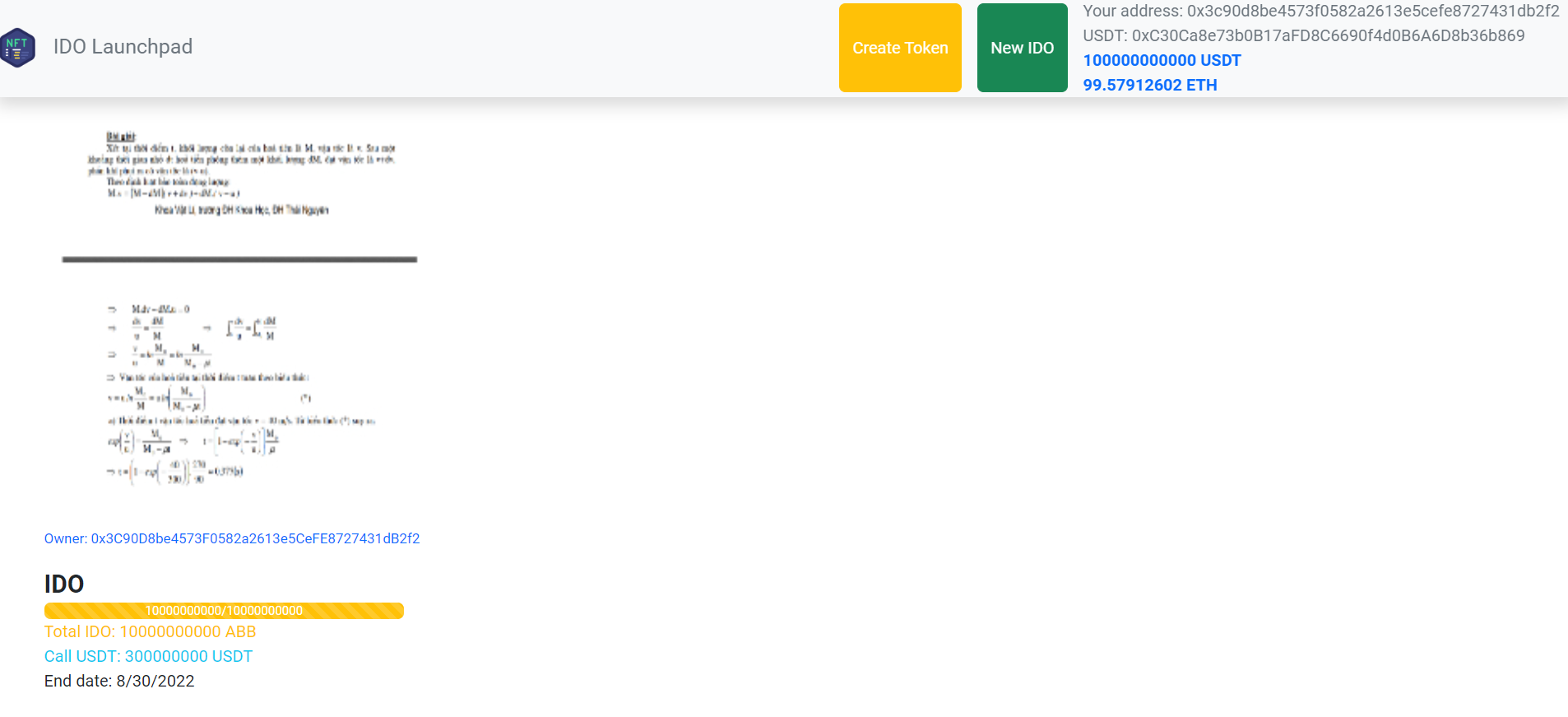
- Ảnh chủ đề của đợt IDO

- Địa chỉ của chủ sở hữu

- Số lượng token tạo cho đợt IDO

- Số lượng USDT max cho đợt IDO

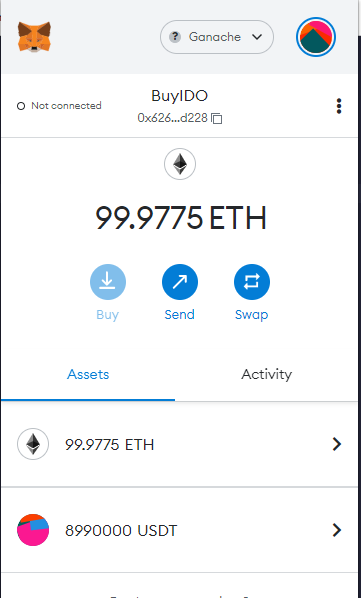
- Thời gian hết hạn đợt IDO



**Hình 24: Giao diện sau khi khởi tạo IDO**

* + 1. **Giao diện người dùng khi buy token từ đợt IDO**

Tạo và sử dụng account thứ 2 (BuyIDO) với tư cách là nhà đầu tư muốn mua token IDO.



**Hình 25: Account nhà đầu tư đã tạo**

Sau khi connect giao diện người dùng khi mua như sau:

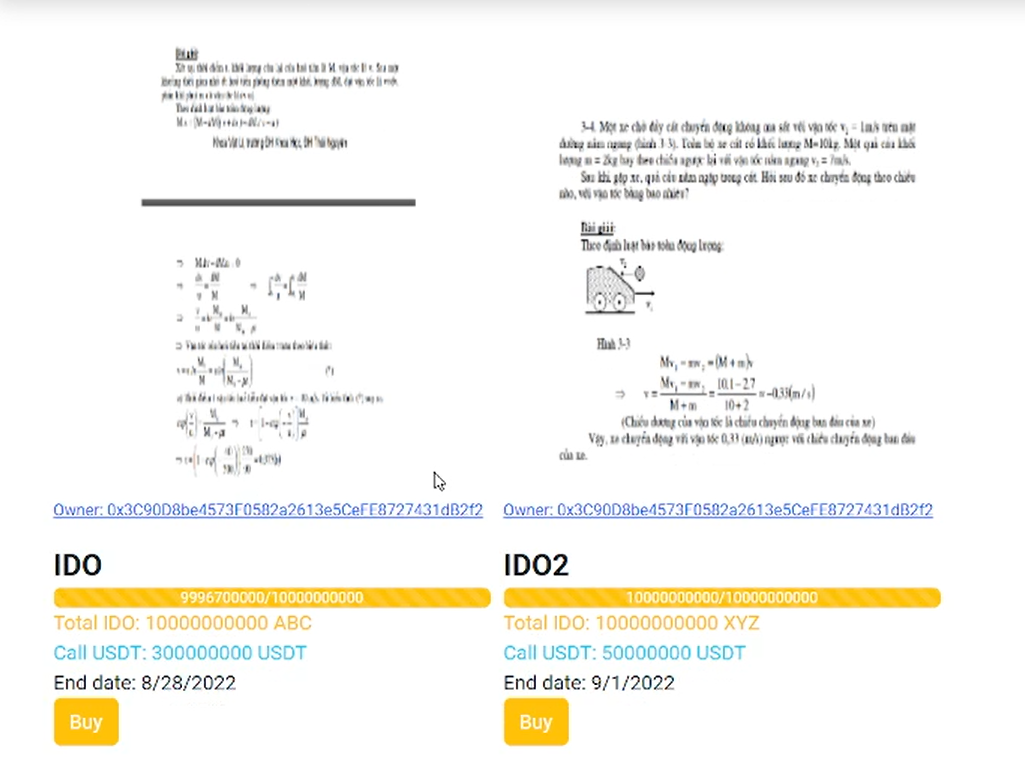
- Địa chỉ của chủ sở hữu

- Số lượng token tạo cho đợt IDO

- Số lượng USDT max cho đợt IDO

- Thời gian hết hạn đợt IDO

- Button buy



**Hình 26: Giao diện người dùng khi mua token IDO**

* + 1. **Giao diện thực hiện buy token**

- Sau khi bấm Buy ở giao diện hình 24, màn hình giao diện ở hình 25 sẽ hiện lên

- Nhập số lượng token USDT muốn dùng để mua lượng token IDO tương ứng

- Số lượng token IDO tương ứng sẽ được hiển thị ngay bên dưới

Các thông tin giao diện bao gồm:

- Địa chỉ của account chủ sở hữu

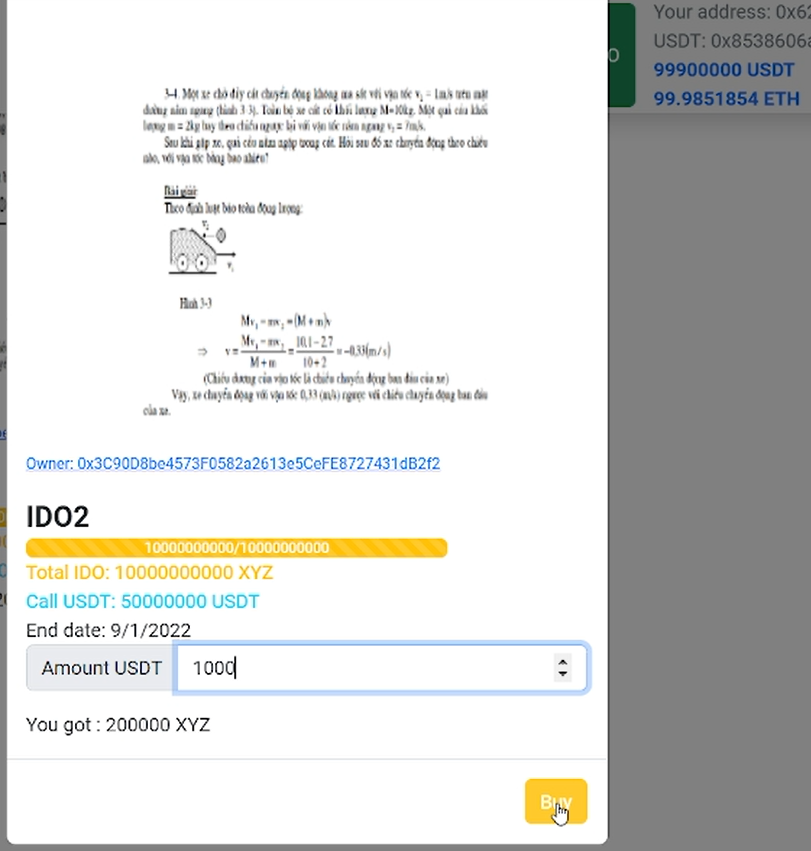
- Số lượng token tạo cho đợt IDO

- Số lượng USDT max cho đợt IDO

- Thời gian hết hạn đợt IDO

- Nhập số lượng USDT dùng để mua

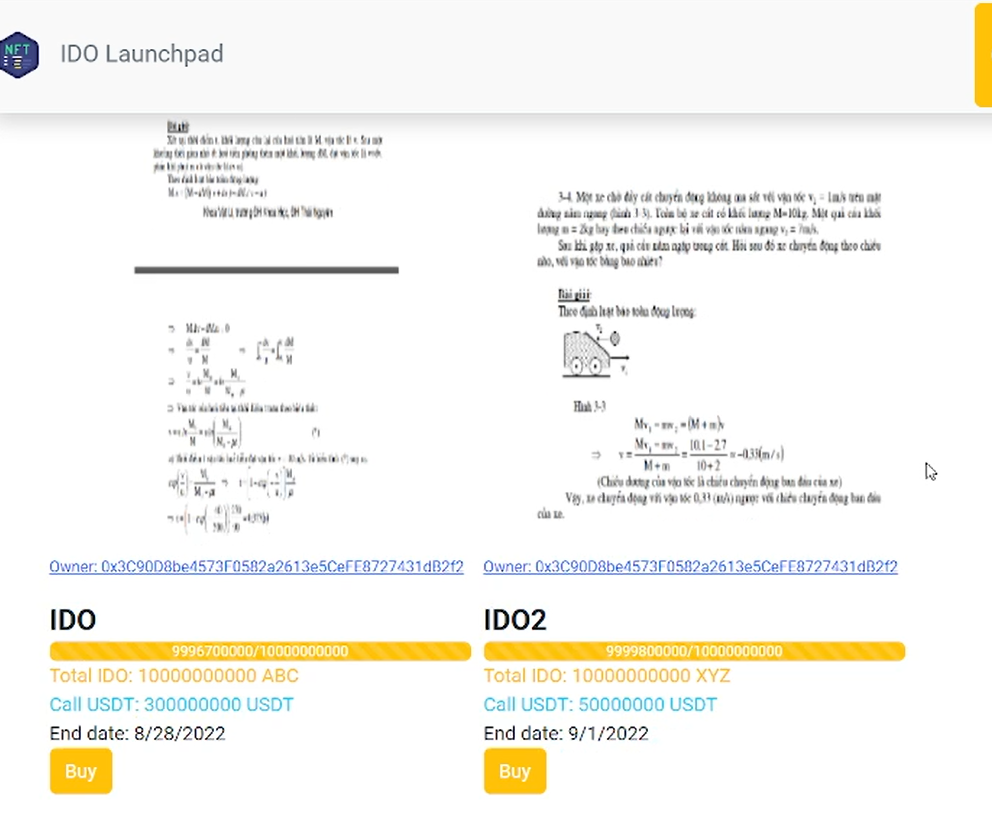
- Hiển thị số lượng token IDO mua được



**Hình 27: Giao diện khi thực hiện mua token IDO**

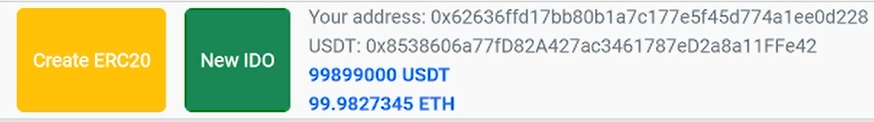
* + 1. **Giao diện sau khi đã mua token IDO thành công**

Sau khi mua thành công số lượng token IDO đã giảm đi



**Hình 28: Giao diện sau khi mua thành công**

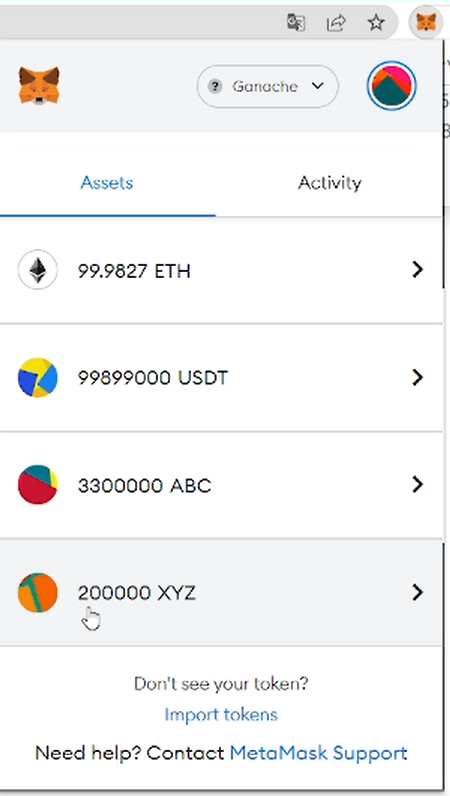
**k) USDT từ wallet đã bị trừ**



**Hình 29: Hiện thị số lượng USDT sau khi mua token IDO**

**l) Kiểm tra wallet và thấy đã mua thành công, token đã chuyển vào wallet**

Để có thể kiểm tra token đã mua. Trước tiên phải import token đó vào wallet



**Hình 30: Số lượng token IDO đã mua**

# KẾT LUẬN

* + - 1. **Kết quả đạt được:**

Từ những hướng dẫn tận tình của thầy, cùng những gì đã học được ở trường,

em đã xây dựng hệ thống launchpad IDO trên nền tảng EVM

với các kết quả đạt được:

* Áp dụng các kiến thức đã học xây dựng website cho phép IDO các token

với giao diện và chức năng khác nhau.

* Quản lý các giao dịch, làm việc với wallet (metamask), tạo các token, tạo các đợt IDO và IDO các token đó.
* Có hầu như đầy đủ chức năng cơ bản để IDO các token.
  + - 1. **Hạn chế:**

Bên cạnh đó cũng có những hạn chế như:

* Chưa có nhiều kiến thức thực tế, nên việc xây dựng phần mềm áp dụng vào

thực tế còn nhiều thiếu sót và chưa khả quan.

* Giao diện chưa thật sự bắt mắt.
* Một số chức năng còn hạn chế.
* Vì đề tài mới được phát triển trong 1-2 năm gần đây nên trong quá trình tìm

hiểu có thể vẫn còn những thiếu sót.

* + - 1. **Hướng phát triển:**

Trong thời gian tới, có thể phát triển luận án đầy đủ hơn, áp dụng vào thực tế:

* Bổ sung thêm nhiều tính năng mới.
* Phát triển, hoàn thiện ứng dụng đầy đủ bám sát vào thực tế hơn.
* Bổ sung hiệu ứng sinh động, hấp dẫn cho trang web, giúp thu hút khách hàng.

# TÀI LIỆU THAM KHẢO

* <https://coinmarketcap.com/alexandria/glossary/initial-dex-offering>
* <https://academy.binance.com/vi/articles/what-is-an-ido-initial-dex-offering>
* <https://coin98.net/what-is-an-ido>
* <https://www.coinbase.com/fr/learn/crypto-basics/what-is-a-token>
* <https://www.finhay.com.vn/token-la-gi>
* <https://ethereum.org/en/developers/docs/dapps/>
* <https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp>
* <https://coin98.net/dapp-la-gi>
* <https://www.coinbase.com/fr/learn/crypto-basics/what-is-a-dex>
* <https://www.gemini.com/cryptopedia/decentralized-exchange-crypto-dex#section-exchanges-of-the-future>
* <https://8thstreetgrille.com/san-dex-la-gi/#:~:text=DEX%20(Decentralized%20Exchange)%20ngh%C4%A9a%20l%C3%A0,t%E1%BB%95%20ch%E1%BB%A9c%20trung%20gian%20n%C3%A0o>.
* <https://ethereum.org/en/>
* <https://www.ibm.com/topics/smart-contracts>
* <https://www.coinbase.com/fr/learn/crypto-basics/what-is-a-smart-contract>
* <https://docs.soliditylang.org/en/v0.8.16/>
* <https://coin98.net/what-is-solidity>
* <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>
* <https://academy.binance.com/vi/articles/what-is-an-ido-initial-dex-offering>
* <https://coinmarketcap.com/alexandria/article/what-is-an-initial-dex-offering-ido-and-why-do-we-need-them>
* <https://academy.binance.com/en/articles/what-is-an-ido-initial-dex-offering>
* <https://www.coindesk.com/learn/what-are-liquidity-pools/>
* https://coin98.net/liquidity-pools-la-gi
* <https://www.dnse.com.vn/hoc/launchpad-la-gi-top-4-nen-tang-launchpad-crypto-pho-bien>
* <https://cryptox100.com/launchpad-trong-crypto-la-gi/>
* <https://reviewinvest.com/web3-la-gi-tong-quan-ve-web3/>
* https://ideausher.com/blog/best-web3-0-frameworks-blockchain/#:~:text=It's%20a%20collection%20of%20tools,such%20as%20forms%20and%20payments.