**Token Creation\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Biên soạn:** Nhóm Nghiên Cứu Blockchain Khoa HTTT

--------------------------------------------------------------------------------------------------------------

1. **Định nghĩa Token**[1], [2]

* Token là một đơn vị tiền ảo được tạo dựa trên nền tảng của một loại tiền ảo khác đã có sẵn trong blockchain để hoạt động.
* **So sánh Token và Coin**

|  |  |  |
| --- | --- | --- |
|  | Token | Coin |
| Tính năng | • Có mục đích sử dụng rộng hơn coin.  • Thường dùng cho các mục đích tiện ích cụ thể (GAS, CMT,..) | • Coin được tạo ra với mục đích sử dụng như tiền tệ.  • Có thể lưu trữ.  • Có thể giao dịch được. |
| Nền tảng | • Phụ thuộc vào nền tảng của coin. | • Có nền tảng riêng. |

* Fungible Token: (FT) Không duy nhất và có thể phân chia. Ví dụ đô la ($) phát hành không duy nhất và có thể phân chia nhỏ ra thành nhiều đơn vị: 1$, 2$, 5$, 10$,…. Trong Ethereum tiêu chuẩn: ERC-20 (Năm 2016)
* Non-fungible Token: (NFT) Là duy nhất và không thể phân chia. Ví dụ vé máy bay là duy nhất và không thể phân chia nhỏ ra được. Trong Ethereum tiêu chuẩn: ERC-721(Năm 2017)
* Multiple Token: (MT) Là sự kết hợp giữa Fungible Token, Non-fungible Token và các loại token khác. Trong Ethereum có tiêu chuẩn ERC-1155 (Năm 2018)

1. **Cài đặt Truffle**

* Để bắt đầu cho Project TokenCreation bước đầu tiên cài đặt Truffle

|  |
| --- |
| npm install -g truffle |

* Khởi tạo Project

|  |
| --- |
| > mkdir <project\_name>  > cd <project\_name>  > truffle unbox react |

Ảnh có chứa văn bản

Mô tả được tạo tự động

1. **Fungible Token (ERC-20)**

* **ERC20 Smart Contrat Installation**

Cài đặt bằng dòng lệnh sau đây:

|  |
| --- |
| npm install --save @openzeppelin/contracts@v3.0.0 |

* **ERC20 Interface**
  + **Các đặc tính của ERC20**
    - **ERC20** cung cấp cơ chế chuyển token từ một tài khoản sang tài khoản khác.
    - Lấy số lượng token hiện tại đang có của một tài khoản.
    - Lấy tổng số lượng token đang sẵn có trong mạng.
    - Chấp thuận nếu số lượng token gửi của một tài khoản có thể sang bên thứ 3.
  + Giải thích cụ thể về ERC20: https://eips.ethereum.org/EIPS/eip-20

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

* **Tạo Contract** MyToken.sol **trong thư mục “truffle/contracts”**

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

* **Migration and Compilation**

Tại thư mục migrations tạo một file js deploy contract có tên là 2\_deploy\_example.js

Ảnh có chứa văn bản

Mô tả được tạo tự động

Với 1000000000 là số lượng Token khởi tạo.

* Vào truffle-config.js thêm compilers thành version sử dụng chung cho toàn bộ contract.

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

* **Tiến hành chạy Migration**

Vào thư mục truffle gõ lệnh

|  |
| --- |
| > truffle develop |

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

|  |
| --- |
| truffle(develop)> migrate |

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

* **Unit Testing MyToken ERC-20**

|  |
| --- |
| npm install --save chai chai-bn chai-as-promised |

Trong thư mục **tests** copy thư mục MyToken.test.js

Gõ lệnh tiếp theo

|  |
| --- |
| truffle test |

Ảnh có chứa văn bản

Mô tả được tạo tự động

* **Tiếp tục test với các hàm khác trong file Test**

**Ảnh có chứa văn bản

Mô tả được tạo tự động**

* **Tạo Crowdsale Contract dùng chung**
  + ICO (Initial Coin Offering) là một hình thức kêu gọi vốn đầu tư khá phổ biến trong các dự án cryptocurrency.
  + Crowdsale là những đợt mở bán Token của một đồng tiền điện tử nào đó trong giai đoạn ICO.
  + Tạo một Contract Crowdsale.sol

Copy Crowdsale template từ <https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v2.5.0/contracts/crowdsale/Crowdsale.sol>

Chỉnh sửa các phần sau đây:

1. Chỉnh sửa Pragma và thư viện

|  |
| --- |
| pragma solidity ^0.5.0;  Chỉnh sửa thành  pragma solidity ^0.6.2;  import "@openzeppelin/contracts/utils/ReentrancyGuard.sol";  import "@openzeppelin/contracts/GSN/Context.sol";  import "@openzeppelin/contracts/token/ERC20/IERC20.sol";  import "@openzeppelin/contracts/math/SafeMath.sol";  import "@openzeppelin/contracts/token/ERC20/SafeERC20.sol"; |

1. Chỉnh sửa fallback function()

|  |
| --- |
| function () external payable {  buyTokens(\_msgSender());  }  Chỉnh sửa thành  receive () external payable {  buyTokens(\_msgSender());  } |

1. Thêm virtual cho những hàm của contract Crowdsale

|  |
| --- |
| Các hàm cần phải thêm virtual  \_preValidatePurchase  \_postValidatePurchase  \_deliverTokens  \_processPurchase  \_updatePurchasingState  \_getTokenAmount |

* **Tạo Crowdsale Contract cá nhân hóa**

Tham khảo file MyTokenSale.sol trong thư mục contract

Ảnh có chứa văn bản

Mô tả được tạo tự động

* **Thay đổi Migrations**

|  |
| --- |
|  |

**Tham khảo file:** 2\_deploy\_example.js

* **Chỉnh sửa lại** MyToken.test.js. **Chạy Unit Test**
* **Tạo file** .env **cho việc sử dụng chung**

Chạy lệnh để cài đặt file **.env**

|  |
| --- |
| npm install --save dotenv |

Tại thư mục gốc thêm thêm file .env

|  |
| --- |
| INITIAL\_TOKENS=10000000 |

Thêm .env vào migrations

|  |
| --- |
| require('dotenv').config({path: './.env'}); |

Thay các thông số thành INITIAL\_TOKENS

* **Contract tiếp theo là KyC Contract**
  + **KYC** được biết đến như là “know your customer” là quy trình để xác định và xác minh danh tính của khách hàng khi tham gia vào mở tài khoản. Nói cách khác, các ngân hàng phải đảm bảo rằng khách hàng của họ thực sự là người mà họ đã đăng ký.
  + **Thực hiện thêm mới KycContract.sol**

Ảnh có chứa văn bản

Mô tả được tạo tự động

* + Thêm KycContract vào migrations
* **Áp dụng Front vào Token Sale App**

1. **Non-fungible Token (ERC-721)**
2. **Multiple Token (ERC-1155)**
3. **Tài liệu tham khảo**

[1] <https://200lab.io/blog/fungible-va-non-fungible-token-su-khac-biet-la-gi/>, [Online] [Thời gian truy cập: 24/06/2022]

[2] <https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/>, [Online] [Thời gian truy cập: 24/06/2022]

[3] <https://www.tutorialspoint.com/solidity/solidity_error_handling.htm>, [Online] [Thời gian truy cập: 23/06/2022]

[4] <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>, [Online]

[Thời gian truy cập: 07/04/2022]