Atelier Web 3.0 n°3: Apprendre à developper une cryptomonnaie et un NFT à l'aide d'un développeur Web 3.0

Sujet

Les bases

▼ Utilisez la bonne version

ℹ️ Il y a différentes versions de Solidity. Pour que le code compile bien, il faut préciser en haut du fichier:

```
pragma solidity ^0.8.0;
```

Ici ^0.8.0 autorise les verison supérieures à 0.8.0 de Solidity.

▼ Créer un contrat (+ constructor)

ℹ️ Un contrat est l'équivalent d'une classe en java ou en C et C++.
Il peut y en avoir plusieurs dans un seul fichier mais par soucis de visibilité, nous vous conseillons de faire un contrat par fichier.
Dans chaque contrat, il y a un unique constructeur.
Le code ci-dessous détaille comment créer un contrat et son constructeur.

```
pragma solidity ^0.8.0;

contract MyFirstContract {

        constructor() public{

        }
}
```

Le mot clé public représente le domaine d'utilisation de la variable ou du constructeur (scope en anglais), c'est à dire dans quelles parties du code on peut l'utiliser ou non.
Pour la déclaration de fonction, il existe différents mot clés: public, internal, external et private, nous ne détaillerons pas ces notions dans cet atelier, nous déclarons toutes les variables et fonctions en public.

▼ Créer une variable

ℹ️ Pour les variables comme pour les fonctions et noms de contrat, on utilise la norme CamelCase, c'est à dire qu'on utilise pas les tirets ou les underscores.
Pour déclarer une variable, on le déclare comme ci-dessus.
Par la même occasion, nous donnons une liste non exhaustive des types de variables:

```
pragma solidity ^0.8.0;

uint nomVariable = 3;

uint256 nomVariable = 3;

bool nomVariable = true;

string CeciEstUneString = 'Hello World';

uint [] public nomVariable = [1, 2, 3, 4, 5];
```

Point important, le mot clé pour les entiers est “uint” et non “int” car les entiers n'existe pas, seules les entiers positifs (unsigned int) existent.

”uint8” : entier non signé qui peut contenir une valeur maximale de 2^8-1. uint8 ne doit utiliser qu'un seul octet d'espace de stockage.

”uint256” entier non signé qui peut contenir une valeur maximale de 2^256-1. uint256 nécessite 32 octets d'espace de stockage.

Attention, les points virgules sont obligatoires en fin de ligne !

▼ Créer une fonction

ℹ️ Une fonction en solidity se crée de la manière suivante:

```
function Name(type parametre1, type parametre2,...)
public view {
        //code de la fonction
}
```

Le mot clé public a la même signification que pour les variables et View indique que l'on ne modifie pas l'état de la blockchain. Cela est le cas seulement pour les getters, lorsqu'une variable change on retire View.

Si la fonction retourne une valeur, on devra préciser le type de la valeur que la fonction retournera :

```
function Name(type parametre1, type parametre2,...)
public view returns(type){
        //code de la fonction
                return //value
}
```

Attention à bien utiliser “returns” dans la déclaration de la fonction et “return” dans le code de la fonction.

1️⃣ Utiliser la version 0.8.20 de Solidity

2️⃣ Créer un contrat WelcomeToSolidity, ajoutez y deux variables: une chaine de caractères “name” et un entier “age”.

3️⃣ Créer le constructeur du contrat qui associe nos deux variables précédentes à deux autres variables prises en paramètre du constructeur.
On rappelle que la convention pour les noms des arguments est de mettre un “_” en premier caractère.
De plus, il ne faut pas oublier de mettre le mot clé “memory” pour une chaîne de caractère exemple “string memory name”

4️⃣ Créer une fonction getMessage qui retourne la chaine de caractères suivante : la variable “name” concaténée avec la chaine de caractère “ fait ses premiers pas en solidity”.

5️⃣ Créer une fonction getResult qui crée deux entiers et retourne la somme des deux.

6️⃣ Créer une fonction sameParity ayant pour paramètre deux entiers. Si les deux entiers ont la même parité, la fonction retourne “true” sinon elle retourne “false”
Indications:
https://solidity-fr.readthedocs.io/fr/latest/types.html

✋ Faites vérifier votre code par Clément, Elie ou Noé

```
pragma solidity ^0.8.20;

contract Member {
        string name;
        uint age;

        //initialiser le nom et l'âge lors du déploiement
        constructor(string memory _name, uint _age) public {
                name = _name;
                                age = _age;
```

```
                }

                function getMessage() public view returns(string
                    string memory intro = " fait ses pre
                    return string.concat(name, intro);
                }

                function getResult() public view returns(uint256
                    uint256 a = 6;
                    uint256 b = 7;
                    return a + b;
                }

                function sameParity(uint256 _number1, uint256 _n
            if(_number1 % 2 == _number2 % 2) {
                return true;
            } else {
                return false;
                }
            }
}
```

Nous allons maintenant rentrer dans le vif du sujet !
Nous vous laissons choisir dans un premier temps entre coder un NFT (Token ERC 721) et une cryptomonnaie (Token ERC 20).
Lorsque que vous avez fini, faites celui que vous n'avez pas choisi et si vous avez le temps, à la fin, se situe une partie bonus mêlant les deux notions.

Enjoy 😉

Développement d'un Token ERC 721

L'objectif ici est de créer un contrat associé à une collection NFT, ce contrat permettra d'obtenir un NFT, le transférer, gérer sa supply et de la connaitre à chaque instant.

1️⃣ Utilisez la version 0.8.20 de Solidity

2️⃣ Importer les librairies via l'url fourni.
Nous vous encourageons à lire le contrat ERC 721 pour se familiariser avec les fonctions si vous le souhaitez.

3️⃣ Créez un contrat MyNFT qui hérite de ERC721.
Pour l'héritage, on utilise le mot clé “is”.

4️⃣ Créez trois variables globales: un entier non signé de taille 256 bits (”uint256”) appelé id, une variable de type “address” appelé owner

5️⃣ Le constructeur du contrat ERC721 prend cette forme:

```
constructor() ERC721("Nom du NFT", "Diminutif") {
        //instructions
    }
```

Dans ce constructeur, associez à la variable owner la personne qui appelle le contrat.

6️⃣ Créer une fonction mint qui permet à celui qui appelle le contrat de récupérer un NFT en utilisant la fonction suivante:

```
_safeMint(address, uint);
_safeMint("variable qui correspond à celui qui appelle le
```

De plus, on souhaite que l'on puisse mint au plus 10 NFT. On vous laisse cherch comment mettre cette condition 😊.

7️⃣ Créer une fonction “getNumberOfNFTMinted” qui retourne le nombre de NFT qui ont été mint

✋ Faites vérifier votre code par Clément, Elie ou Noé.

▼ **Code de base pour un NFT**

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";

contract MyNFT is ERC721 {
    uint256 id;
    address owner;

    constructor() ERC721("MyNFT", "NFT") {
        owner = msg.sender;
    }

    function mint() public {
        require(id <= 9);
        _safeMint(msg.sender, id);
        id++;
    }

        function getNumberOfNFTMinted() public view returns(u
        return id;
    }
}
```

Développement d'un Token ERC 20

L'objectif de cette partie est de créer un jeton avec une supply de notre choix, de le transférer à une adresse, de mint le token et de changer le possesseur du contrat.

1️⃣ Utilisez la version 0.8.20 de Solidity

2️⃣ Importer les librairies via l'url fourni.
Nous vous encourageons à lire le contrat ERC 20 pour se familiariser avec les fonctions si vous le souhaitez.

3️⃣ Créez un contrat MyToken qui hérite de ERC20.

4️⃣ Créez deux variables globales: un entier non signé de taille 256 bits appelé *_initial_*supply, une variable de type “address” public appelé owner. Affectez à l'entier non signé la supply que vous voulez.
Attention, on veut que notre token ait 18 décimales pour cela sous la forme uint : 1 token = 10 ** 18

5️⃣ Le constructeur du contrat ERC20 prend la même forme que celui de l'ERC 721.

Dans ce constructeur, associez à la variable owner la personne qui appelle le contrat et utilise la fonction du contrat ERC 20 qui permet de Mint, l'instruction doit permettre à la personne qui appelle le contrat de Mint toute la supply.

6️⃣ Créer une fonction Mint ayant pour argument une variable de type address et un unsigned int : uint. Cette fonction s'assure que l'owner est bien celui qui appelle le contrat et qui utilise la fonction Mint du contrat ERC 20 avec les arguments de la fonction.

7️⃣ Créer une fonction changeOwner qui a pour argument une address, celle-ci s'assure que l'owner est bien la personne qui appelle le contrat.
Cette fonction associé à la variable owner le paramètre de la fonction.

✋ Faites vérifier votre code par Clément, Elie ou Noé.

▼ **Code de base pour un token**

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract TokenTest is ERC20 {
    uint _initial_supply = 100000 * (10 ** 18);
    address public owner; // ON A RAJOUTE UN OWNER

    constructor() ERC20("TokenTest", "TKN") {
        _mint(msg.sender, _initial_supply);
        owner = msg.sender; // ON DECLARE ICI QUE OWNER SERA
    }

        modifier onlyOwner { // Leur expliquer qu'on peut uti
                require(msg.sender == owner);
                _;
        }

    function mint(address to, uint256 amount) public {
        require(owner == msg.sender); // SEULEMENT OWNER PEUT
        _mint(to, amount);
    }

    function changeOwner(address _owner) public {
        require(owner == msg.sender);
        owner = _owner;
    }
```

Bonus

❔ Rajouter une variable bool “trading”, lorsque cette variable est égale à “false”, seul l’owner peut appeler la fonction _transfer.
Ensuite, faites une fonction qui met la variable “trading” égale à true. Cette fonction ne peut être appelée que par l’owner.

```
bool isTradingLive;

function enableTrading(bool _trading) external {
                require(msg.sender == owner);
        isTradingLive = _trading;
    }
```

❔ Rajouter 2 variables :

- maxWallet : nombre de tokens maximum qu'une personne peut posséder.
- maxAmount : montant de token maximum par transaction

Rajouter une variable "tax" qui correspond à un % de chaque transaction qui ira dans le wallet de l'owner.
Exemple : si tax = 5 alors 5% de chaque transaction ira dans le wallet de l'owner.

Modifier la fonction _transfer :

Aller dans le contrat ERC20.sol que l'on a importé, puis au niveau de la fonction "_transfer()" ajouter le mot clé "virtual" après le mot clé "internal"

Dans notre contrat, écrivez la fonction _transfer comme cela :

```
function _transfer(address from, address to,uint256 amount
        //modification que l'on veut apporter
        super._transfer(from, to, amount); //appel de la f
}
```

Le mot clé "override" permet de modifier la fonction _transfer du contrat ERC20.s

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract TokenTest is ERC20 {
    uint _initial_supply = 100000 * (10 ** 18);
    address public owner; // ON A RAJOUTE UN OWNER
    uint256 public maxAmount = 10_000e18;
    uint256 public maxWallet = 15_000e18;
    uint256 public tax = 5;
    bool public isTradingLive;
```

```
    constructor() ERC20("TokenTest", "TKN") {
        _mint(msg.sender, _initial_supply);
        owner = msg.sender; // ON DECLARE ICI QUE OWNER SERA L'A
    }

    function mint(address to, uint256 amount) public {
        require(owner == msg.sender); // SEULEMENT OWNER PEUT AP
        _mint(to, amount);
    }

    function changeOwner(address _owner) public {
        require(owner == msg.sender);
        owner = _owner;
    }

    function enableTrading(bool _trading) external {
        require(msg.sender == owner);
        isTradingLive = _trading;
    }

    function _transfer(address from, address to,uint256 amount)
        if(from != owner) {
        require(isTradingLive, "Trading is not open yet");
        }
        require(amount + balanceOf(to) <= maxWallet, "Max Wallet
        require(amount <= maxAmount, "Max amount");

        uint256 taxAmount = (amount * tax) / 100;
        amount -= taxAmount;
        super._transfer(from, owner, taxAmount);
        super._transfer(from, to, amount);
    }
}
```

Lien entre token et NFT

❔ Déployer le contrat du NFT précédemment réalisé

❔ Créer un contrat Token et importer les contrats suivants :

- ERC20.sol
- ERC721.sol
- IUniswapV2Factory.sol
- IUniswapV2Router02.sol

❔ Récupérez l’adresse du contrat NFT que vous avez déployé et créez une variable “NFT” de type address qui sera égale à l’adresse du contrat NFT

❔ Modifier la fonction _beforeTokenTransfer(from, to, amount) du contrat ERC20 de sorte à ce que :

- si “from” ou “to” n'est pas le owner, il faut que “from” ou “to” possède le NFT.

❔ Ecrire une fonction doesUserHasNFT qui prend une adresse en paramètre et renvoie “true” si l’adresse possède le NFT et “false” sinon

▼ **Token qui nécessite la détention d’un NFT pour être transféré**

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol"; //con
import "@openzeppelin/contracts/token/ERC721/IERC721.sol"; //
import "interfaces/IUniswapV2Factory.sol"; // contrat Uniswap
import "interfaces/IUniswapV2Router02.sol"; // contrat Router
```

```
contract Token is ERC20 {
    uint constant _initial_supply = 100000 * (10 ** 18);

    address public owner;
    address public sennder; // servira pour la fonction _befo
    uint256 public _amount; // servira pour la fonction _befo
    address public receiver; // servira pour la fonction _bef
    address NFT = 0x78dc396dFA93CF1d585669c2B3Cabf83Fe12b212;

    mapping(address => bool) public exempt; // owner sera exe

    address public lpPair; // adresse de la paire Token / WET
    IUniswapV2Router02 public uniRouter;
    address _uniswap;

    constructor() ERC20("TokenTest", "TKN") {
        exempt[msg.sender] = true; // exclut l'owner, il n'au
        _mint(msg.sender, _initial_supply); // mint la total
        owner = msg.sender;

        _uniswap = 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D
        uniRouter = IUniswapV2Router02(_uniswap);
        lpPair = IUniswapV2Factory(uniRouter.factory()).creat
            address(this),
            uniRouter.WETH()
        );
    }

    function _beforeTokenTransfer( // modification de la fonc
        address from,
        address to,
        uint256 amount
    ) internal override {
        if (!exempt[from] && !exempt[to]) { // si from ou to
            require(
                IERC721(NFT).balanceOf(to) > 0 ||
                    IERC721(NFT).balanceOf(from) > 0,
                "You need NFT"
            );
```

```
        } else {
            sennder = from;
            receiver = to;
            _amount = amount;
        }
    }

    function mint(address to, uint256 amount) public {
        require(owner == msg.sender);
        _mint(to, amount);
    }

    function exemptAddress(address _address) external {
        exempt[_address] = true;
    }

    function changeOwner(address _owner) public {
        require(owner == msg.sender);
        owner = _owner;
    }

    function isUserHasNFT(address _address) external view ret
        if (IERC721(NFT).balanceOf(_address) > 0) {
            return true;
        } else {
            return false;
        }
    }
}
```

Code vide :

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol"; //contra
import "@openzeppelin/contracts/token/ERC721/IERC721.sol"; //int
import "interfaces/IUniswapV2Factory.sol"; // contrat Uniswap po
import "interfaces/IUniswapV2Router02.sol"; // contrat Router Un
```

```
contract Token is ERC20 {
    uint constant _initial_supply = 100000 * (10 ** 18);

    address public owner;
    address public sennder; // servira pour la fonction _beforeT
    uint256 public _amount; // servira pour la fonction _beforeT
    address public receiver; // servira pour la fonction _before
    address NFT = ; // adresse du contrat NFT

    mapping(address => bool) public exempt; // owner sera exempt

    address public lpPair; // adresse de la paire Token / WETH
    IUniswapV2Router02 public uniRouter;
    address _uniswap;

    constructor() ERC20("TokenTest", "TKN") {
        exempt[msg.sender] = true; // exclut l'owner, il n'aura
        _mint(msg.sender, _initial_supply); // mint la total sup
        owner = msg.sender;

        _uniswap = 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D; /
        uniRouter = IUniswapV2Router02(_uniswap);
        lpPair = IUniswapV2Factory(uniRouter.factory()).createPa
            address(this),
            uniRouter.WETH()
        );
    }

    function _beforeTokenTransfer( // modification de la fonctio
        address from,
        address to,
        uint256 amount
    ) internal override {
        //...
          sennder = from;
          receiver = to;
          _amount = amount;

    }
```

```
    function mint(address to, uint256 amount) public {
        require(owner == msg.sender);
        _mint(to, amount);
    }

    function exemptAddress(address _address) external {
        exempt[_address] = true;
    }

    function changeOwner(address _owner) public {
        require(owner == msg.sender);
        owner = _owner;
    }

    function doesUserHasNFT(address _address) external view retu
        //...
    }
}
```

▼ **Contrats**

▼ ERC20

```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts (last updated v4.9.0) (token/ERC

pragma solidity ^0.8.0;

import "./IERC20.sol";
import "./extensions/IERC20Metadata.sol";
import "../../utils/Context.sol";

/**
 * @dev Implementation of the {IERC20} interface.
 *
 * This implementation is agnostic to the way tokens are c
 * that a supply mechanism has to be added in a derived co
 * For a generic mechanism see {ERC20PresetMinterPauser}.
```

```
 *
 * TIP: For a detailed writeup see our guide
 * https://forum.openzeppelin.com/t/how-to-implement-erc20
 * to implement supply mechanisms].
 *
 * The default value of {decimals} is 18. To change this,
 * this function so it returns a different value.
 *
 * We have followed general OpenZeppelin Contracts guideli
 * instead returning `false` on failure. This behavior is
 * conventional and does not conflict with the expectation
 * applications.
 *
 * Additionally, an {Approval} event is emitted on calls t
 * This allows applications to reconstruct the allowance f
 * by listening to said events. Other implementations of t
 * these events, as it isn't required by the specification
 *
 * Finally, the non-standard {decreaseAllowance} and {incr
 * functions have been added to mitigate the well-known is
 * allowances. See {IERC20-approve}.
 */
contract ERC20 is Context, IERC20, IERC20Metadata {
    mapping(address => uint256) private _balances;

    mapping(address => mapping(address => uint256)) privat

    uint256 private _totalSupply;

    string private _name;
    string private _symbol;

    /**
     * @dev Sets the values for {name} and {symbol}.
     *
     * All two of these values are immutable: they can onl
     * construction.
     */
    constructor(string memory name_, string memory symbol_
        _name = name_;
```

```
        _symbol = symbol_;
    }

    /**
     * @dev Returns the name of the token.
     */
    function name() public view virtual override returns (
        return _name;
    }

    /**
     * @dev Returns the symbol of the token, usually a sho
     * name.
     */
    function symbol() public view virtual override returns
        return _symbol;
    }

    /**
     * @dev Returns the number of decimals used to get its
     * For example, if `decimals` equals `2`, a balance of
     * be displayed to a user as `5.05` (`505 / 10 ** 2`).
     *
     * Tokens usually opt for a value of 18, imitating the
     * Ether and Wei. This is the default value returned b
     * it's overridden.
     *
     * NOTE: This information is only used for _display_ p
     * no way affects any of the arithmetic of the contrac
     * {IERC20-balanceOf} and {IERC20-transfer}.
     */
    function decimals() public view virtual override retur
        return 18;
    }

    /**
     * @dev See {IERC20-totalSupply}.
     */
    function totalSupply() public view virtual override re
        return _totalSupply;
```

```
    }

    /**
     * @dev See {IERC20-balanceOf}.
     */
    function balanceOf(address account) public view virtua
        return _balances[account];
    }

    /**
     * @dev See {IERC20-transfer}.
     *
     * Requirements:
     *
     * - `to` cannot be the zero address.
     * - the caller must have a balance of at least `amoun
     */
    function transfer(address to, uint256 amount) public v
        address owner = _msgSender();
        _transfer(owner, to, amount);
        return true;
    }

    /**
     * @dev See {IERC20-allowance}.
     */
    function allowance(address owner, address spender) pub
        return _allowances[owner][spender];
    }

    /**
     * @dev See {IERC20-approve}.
     *
     * NOTE: If `amount` is the maximum `uint256`, the all
     * `transferFrom`. This is semantically equivalent to
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     */
```

```
    function approve(address spender, uint256 amount) publ
        address owner = _msgSender();
        _approve(owner, spender, amount);
        return true;
    }

    /**
     * @dev See {IERC20-transferFrom}.
     *
     * Emits an {Approval} event indicating the updated al
     * required by the EIP. See the note at the beginning
     *
     * NOTE: Does not update the allowance if the current
     * is the maximum `uint256`.
     *
     * Requirements:
     *
     * - `from` and `to` cannot be the zero address.
     * - `from` must have a balance of at least `amount`.
     * - the caller must have allowance for ``from``'s tok
     * `amount`.
     */
    function transferFrom(address from, address to, uint25
        address spender = _msgSender();
        _spendAllowance(from, spender, amount);
        _transfer(from, to, amount);
        return true;
    }

    /**
     * @dev Atomically increases the allowance granted to
     *
     * This is an alternative to {approve} that can be use
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated al
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
```

```
     */
    function increaseAllowance(address spender, uint256 ad
        address owner = _msgSender();
        _approve(owner, spender, allowance(owner, spender)
        return true;
    }

    /**
     * @dev Atomically decreases the allowance granted to
     *
     * This is an alternative to {approve} that can be use
     * problems described in {IERC20-approve}.
     *
     * Emits an {Approval} event indicating the updated al
     *
     * Requirements:
     *
     * - `spender` cannot be the zero address.
     * - `spender` must have allowance for the caller of a
     * `subtractedValue`.
     */
    function decreaseAllowance(address spender, uint256 su
        address owner = _msgSender();
        uint256 currentAllowance = allowance(owner, spende
        require(currentAllowance >= subtractedValue, "ERC2
        unchecked {
            _approve(owner, spender, currentAllowance - su
        }

        return true;
    }

    /**
     * @dev Moves `amount` of tokens from `from` to `to`.
     *
     * This internal function is equivalent to {transfer},
     * e.g. implement automatic token fees, slashing mecha
     *
     * Emits a {Transfer} event.
     *
```

```
     * Requirements:
     *
     * - `from` cannot be the zero address.
     * - `to` cannot be the zero address.
     * - `from` must have a balance of at least `amount`.
     */
    function _transfer(address from, address to, uint256 a
        require(from != address(0), "ERC20: transfer from
        require(to != address(0), "ERC20: transfer to the

        _beforeTokenTransfer(from, to, amount);

        uint256 fromBalance = _balances[from];
        require(fromBalance >= amount, "ERC20: transfer am
        unchecked {
            _balances[from] = fromBalance - amount;
            // Overflow not possible: the sum of all balan
            // decrementing then incrementing.
            _balances[to] += amount;
        }

        emit Transfer(from, to, amount);

        _afterTokenTransfer(from, to, amount);
    }

    /** @dev Creates `amount` tokens and assigns them to `
     * the total supply.
     *
     * Emits a {Transfer} event with `from` set to the zer
     *
     * Requirements:
     *
     * - `account` cannot be the zero address.
     */
    function _mint(address account, uint256 amount) intern
        require(account != address(0), "ERC20: mint to the

        _beforeTokenTransfer(address(0), account, amount);
```

```
        _totalSupply += amount;
        unchecked {
            // Overflow not possible: balance + amount is
            _balances[account] += amount;
        }
        emit Transfer(address(0), account, amount);

        _afterTokenTransfer(address(0), account, amount);
    }

    /**
     * @dev Destroys `amount` tokens from `account`, reduc
     * total supply.
     *
     * Emits a {Transfer} event with `to` set to the zero
     *
     * Requirements:
     *
     * - `account` cannot be the zero address.
     * - `account` must have at least `amount` tokens.
     */
    function _burn(address account, uint256 amount) intern
        require(account != address(0), "ERC20: burn from t

        _beforeTokenTransfer(account, address(0), amount);

        uint256 accountBalance = _balances[account];
        require(accountBalance >= amount, "ERC20: burn amo
        unchecked {
            _balances[account] = accountBalance - amount;
            // Overflow not possible: amount <= accountBal
            _totalSupply -= amount;
        }

        emit Transfer(account, address(0), amount);

        _afterTokenTransfer(account, address(0), amount);
    }

    /**
```

```
     * @dev Sets `amount` as the allowance of `spender` ov
     *
     * This internal function is equivalent to `approve`,
     * e.g. set automatic allowances for certain subsystem
     *
     * Emits an {Approval} event.
     *
     * Requirements:
     *
     * - `owner` cannot be the zero address.
     * - `spender` cannot be the zero address.
     */
    function _approve(address owner, address spender, uint
        require(owner != address(0), "ERC20: approve from
        require(spender != address(0), "ERC20: approve to

        _allowances[owner][spender] = amount;
        emit Approval(owner, spender, amount);
    }

    /**
     * @dev Updates `owner` s allowance for `spender` base
     *
     * Does not update the allowance amount in case of inf
     * Revert if not enough allowance is available.
     *
     * Might emit an {Approval} event.
     */
    function _spendAllowance(address owner, address spende
        uint256 currentAllowance = allowance(owner, spende
        if (currentAllowance != type(uint256).max) {
            require(currentAllowance >= amount, "ERC20: in
            unchecked {
                _approve(owner, spender, currentAllowance
            }
        }
    }

    /**
     * @dev Hook that is called before any transfer of tok
```

```
     * minting and burning.
     *
     * Calling conditions:
     *
     * - when `from` and `to` are both non-zero, `amount`
     * will be transferred to `to`.
     * - when `from` is zero, `amount` tokens will be mint
     * - when `to` is zero, `amount` of ``from``'s tokens
     * - `from` and `to` are never both zero.
     *
     * To learn more about hooks, head to xref:ROOT:extend
     */
    function _beforeTokenTransfer(address from, address to

    /**
     * @dev Hook that is called after any transfer of toke
     * minting and burning.
     *
     * Calling conditions:
     *
     * - when `from` and `to` are both non-zero, `amount`
     * has been transferred to `to`.
     * - when `from` is zero, `amount` tokens have been mi
     * - when `to` is zero, `amount` of ``from``'s tokens
     * - `from` and `to` are never both zero.
     *
     * To learn more about hooks, head to xref:ROOT:extend
     */
    function _afterTokenTransfer(address from, address to,
}
```

▼ ERC721

```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts (last updated v4.9.0) (token/ERC

pragma solidity ^0.8.0;

import "../../utils/introspection/IERC165.sol";
```

```
/**
 * @dev Required interface of an ERC721 compliant contract
 */
interface IERC721 is IERC165 {
    /**
     * @dev Emitted when `tokenId` token is transferred fr
     */
    event Transfer(address indexed from, address indexed t

    /**
     * @dev Emitted when `owner` enables `approved` to man
     */
    event Approval(address indexed owner, address indexed

    /**
     * @dev Emitted when `owner` enables or disables (`app
     */
    event ApprovalForAll(address indexed owner, address in

    /**
     * @dev Returns the number of tokens in ``owner``'s ac
     */
    function balanceOf(address owner) external view return

    /**
     * @dev Returns the owner of the `tokenId` token.
     *
     * Requirements:
     *
     * - `tokenId` must exist.
     */
    function ownerOf(uint256 tokenId) external view return

    /**
     * @dev Safely transfers `tokenId` token from `from` t
     *
     * Requirements:
     *
     * - `from` cannot be the zero address.
     * - `to` cannot be the zero address.
```

```
     * - `tokenId` token must exist and be owned by `from`
     * - If the caller is not `from`, it must be approved
     * - If `to` refers to a smart contract, it must imple
     *
     * Emits a {Transfer} event.
     */
    function safeTransferFrom(address from, address to, ui

    /**
     * @dev Safely transfers `tokenId` token from `from` t
     * are aware of the ERC721 protocol to prevent tokens
     *
     * Requirements:
     *
     * - `from` cannot be the zero address.
     * - `to` cannot be the zero address.
     * - `tokenId` token must exist and be owned by `from`
     * - If the caller is not `from`, it must have been al
     * - If `to` refers to a smart contract, it must imple
     *
     * Emits a {Transfer} event.
     */
    function safeTransferFrom(address from, address to, ui

    /**
     * @dev Transfers `tokenId` token from `from` to `to`.
     *
     * WARNING: Note that the caller is responsible to con
     * or else they may be permanently lost. Usage of {saf
     * understand this adds an external call which potenti
     *
     * Requirements:
     *
     * - `from` cannot be the zero address.
     * - `to` cannot be the zero address.
     * - `tokenId` token must be owned by `from`.
     * - If the caller is not `from`, it must be approved
     *
     * Emits a {Transfer} event.
     */
```

```
    function transferFrom(address from, address to, uint25

    /**
     * @dev Gives permission to `to` to transfer `tokenId`
     * The approval is cleared when the token is transferr
     *
     * Only a single account can be approved at a time, so
     *
     * Requirements:
     *
     * - The caller must own the token or be an approved o
     * - `tokenId` must exist.
     *
     * Emits an {Approval} event.
     */
    function approve(address to, uint256 tokenId) external

    /**
     * @dev Approve or remove `operator` as an operator fo
     * Operators can call {transferFrom} or {safeTransferF
     *
     * Requirements:
     *
     * - The `operator` cannot be the caller.
     *
     * Emits an {ApprovalForAll} event.
     */
    function setApprovalForAll(address operator, bool appr

    /**
     * @dev Returns the account approved for `tokenId` tok
     *
     * Requirements:
     *
     * - `tokenId` must exist.
     */
    function getApproved(uint256 tokenId) external view re

    /**
     * @dev Returns if the `operator` is allowed to manage
```

```
     *
     * See {setApprovalForAll}
     */
    function isApprovedForAll(address owner, address opera
}
```

▼ IERC165

```
// SPDX-License-Identifier: MIT
// OpenZeppelin Contracts v4.4.1 (utils/introspection/IERC

pragma solidity ^0.8.0;

/**
 * @dev Interface of the ERC165 standard, as defined in th
 * https://eips.ethereum.org/EIPS/eip-165[EIP].
 *
 * Implementers can declare support of contract interfaces
 * queried by others ({ERC165Checker}).
 *
 * For an implementation, see {ERC165}.
 */
interface IERC165 {
    /**
     * @dev Returns true if this contract implements the i
     * `interfaceId`. See the corresponding
     * https://eips.ethereum.org/EIPS/eip-165#how-interfac
     * to learn more about how these ids are created.
     *
     * This function call must use less than 30 000 gas.
     */
    function supportsInterface(bytes4 interfaceId) externa
}
```

▼ IUniswapV2Factory

```
pragma solidity ^0.8.0;

interface IUniswapV2Factory {
    function createPair(
```

```
        address tokenA,
        address tokenB
    ) external returns (address pair);
}
```

▼ IUniswapV2Router02

```
pragma solidity ^0.8.0;

interface IUniswapV2Router02 {
    function factory() external pure returns (address);

    function WETH() external pure returns (address);

    function swapExactTokensForETHSupportingFeeOnTransferT
        uint amountIn,
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external;

    function swapExactETHForTokensSupportingFeeOnTransferT
        uint amountOutMin,
        address[] calldata path,
        address to,
        uint deadline
    ) external payable;

    function getAmountsOut(
        uint amountIn,
        address[] calldata path
    ) external view returns (uint[] memory amounts);

    function getAmountsIn(
        uint amountOut,
        address[] calldata path
    ) external view returns (uint[] memory amounts);
}
```