



리액트로 구현하는 이더리움 ERC-721



1. ERC-721 표준

- ERC721 메인 인터페이스

```
pragma solidity ^0.4.20;

/// @title ERC-721 Non-Fungible Token Standard
/// @dev See https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md
/// Note: the ERC-165 identifier for this interface is 0x80ac58cd.

interface ERC721 /* is ERC165 */ {

    event Transfer(address indexed _from, address indexed _to, uint256 indexed _tokenId);
    event Approval(address indexed _owner, address indexed _approved, uint256 indexed _tokenId);
    event ApprovalForAll(address indexed _owner, address indexed _operator, bool _approved);

    function balanceOf(address _owner) external view returns (uint256);
    function ownerOf(uint256 _tokenId) external view returns (address);
    function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data) external payable;
    function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
    function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
    function approve(address _approved, uint256 _tokenId) external payable;
    function setApprovalForAll(address _operator, bool _approved) external;
    function getApproved(uint256 _tokenId) external view returns (address);
    function isApprovedForAll(address _owner, address _operator) external view returns (bool);
}

interface ERC165 {
    function supportsInterface(bytes4 interfaceID) external view returns (bool);
}
```

1. ERC-721 표준

- ERC165

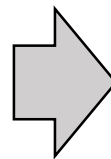
컨트랙트가 표준 인터페이스를 구현한 것인지 확인하기 위한 "Standard Interface Detection"

```
interface ERC165 {  
    function supportsInterface(bytes4 interfaceID) external view returns (bool);  
}
```

[구현 예제]

ERC-721표준 인터페이스를 구현하는 컨트랙트는 ERC-165를 구현하여 그 여부를 확인할 수 있어야 한다.

```
this.balanceOf.selector ^  
this.ownerOf.selector ^  
bytes4(keccak256("safeTransferFrom(address,address,uint256)")) ^  
bytes4(keccak256("safeTransferFrom(address,address,uint256,bytes)")) ^  
this.transferFrom.selector ^  
this.approve.selector ^  
this.setApprovalForAll.selector ^  
this.getApproved.selector ^  
this.isApprovedForAll.selector
```



0x80ac58cd

각 함수 selector의 XOR연산

1. ERC-721 표준

- ERC165

```
supportedInterfaces[0x80ac58cd] = true; //ERC721
```

```
function supportsInterface(bytes4 interfaceID) external view returns (bool){  
    return supportedInterfaces[interfaceID];  
}
```

1. ERC-721 표준

- ERC721

3개의 이벤트 - 이벤트 발생시 화면(UI)에 알림용

Transfer : 소유권 이전시 발생

Approval : 소유권 이전 승인시 발생(하나의 토큰)

ApprovalForAll : 소유권 이전 승인시 발생(모든 토큰)

1. ERC-721 표준

- ERC721

9개의 함수

`balanceOf(address _owner)` : 소유 계정의 토큰 수

`ownerOf(uint256 _tokenId)` : 토큰의 소유 계정

`safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data)`

`safeTransferFrom(address _from, address _to, uint256 _tokenId)`

: 소유권 이전, `_to`가 컨트랙트일 때(`code size > 0`)는 그 컨트랙트의 `onERC721Received` 함수를 호출하여 그것이 함수 `selector`와 일치하는지 확인

`transferFrom(address _from, address _to, uint256 _tokenId)` : 소유권 이전

“THE CALLER IS RESPONSIBLE TO CONFIRM THAT”

토큰 소유계정

1. ERC-721 표준

- ERC721

`approve(address _approve, uint256 _token_id)` : 소유권 이전 승인 계정 지정(토큰 하나)

`setApproveForAll(address _operator, bool _approved)` : 소유권 이전 승인 계정 지정(토큰 모두)

`getApproved(uint256 _tokenId)` : 소유권 이전 승인 계정 조회

`isApprovedForAll(address _owner, address _operator)` : 소유권 이전 승인 여부 조회


1. ERC-721 표준

- ERC721Enumerable

`totalSupply()` : 발행된 유효한 토큰 수

`tokenByIndex(uint256 _index)` : `_index`에 해당하는 토큰ID 인덱스는 `_index < totalSupply()`

인덱스	자산ID(토큰ID)
0	240609
1	145598
2	445109

인덱스	자산ID(토큰ID)
2 	445109

`tokenOfOwnerByIndex(address _owner, uint256 _index)` : 소유 계정이 가진 토큰 중 인덱스에 해당하는 토큰ID

1. ERC-721 표준

- ERC721Metadata

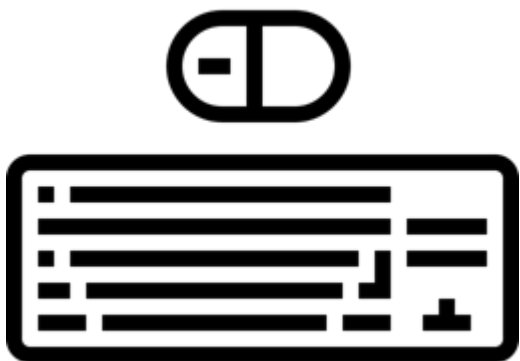
name() : 토큰 이름

symbol() : 토큰 심볼

tokenURI(uint256 _tokenId) : 토큰 ID가 가리키는 리소스 정보(JSON)

[예] {
 "title": "Asset Metadata",
 "type": "object",
 "properties": {
 "name": {
 "type": "string",
 "description": "Identifies the asset to which this NFT represents"
 },
 "description": {
 "type": "string",
 "description": "Describes the asset to which this NFT represents"
 },
 "image": {
 "type": "string",
 "description": "A URI pointing to a resource with mime type image/* representing the asset to which this NFT represents. Consider making any images at a width between 320 and 1080 pixels and aspect ratio between 1.91:1 and 4:5 inclusive."
 }
 }
}

다음 시간에는...



- ERC-721 컨트랙트 구현

