

This is an instantiation of a proof-of-concept to illustrate an NFT mechanism for which the tokens have multiple owners, that have different share percentages over the token. The code consists of two parts:

- A javascript frontend interacting with the ethereum blockchain using the web3 API.
- Implementation of contract logic in Solidity.

In short, the solidity code resides in *Explorer.sol* and is represented by two contracts: *ExplorerToken* and *ExplorerSupply*. *ExplorerToken* (1) represents an "internal" contract and is responsible for keeping track of the tokens themselves and their properties. *ExplorerSupply* (2) is the contract that is meant to interact with the "exterior" and mainly wraps the creation method for the tokens from *ExplorerToken*.

Besides the above mentioned contracts, a significant part of functionality is given by the (openzeppelin) contracts that are being inherited:

- *Ownable* provides a mechanism by which the contracts have an owner that has exclusive access to some specific functionality, in our case being the creation of new tokens.
- *Counters* library exposes a restrictive and (more) secure implementation of a counter, used for keeping track of the tokens created.
- *ERC721Enumerable* is an extension of ERC721 standard (NFTs) that originally permit the creation of non fungible tokens, and provided means of transferring them across (authorised) blockchain addresses. The "enumerable" extension permits indexing tokens, feature used for the frontend module.
- *ERC1155* is a contract that implements the standard with the same name, which allows to have multiple token types with one / more units for each. In this particular case, it is used to keep track of each token's shares distribution among multiple owners.
- *IERC721Receiver* is an interface, that, according to openzeppelin documentation, it is necessary for implementing a standardised way of receiving ERC721 tokens.

The functionality itself is provided by combining the *ERC721* and *ERC1155* functionality: when a new location token is created, it is first "minted" in the *ExplorerToken*, then it is also "minted" in the *ERC1155* - this poses the disadvantage of spending more gas per token, and also the need for synchronising the two contract states arises.

The javascript component uses web3 API to interact with the blockchain and with the contracts' method themselves:

- *web3.eth.Contract()* to "cast" a given address to the contract type that is used (in our case, the *ExplorerSupply* and *ExplorerToken* instances)
- *ExplorerToken.totalSupply().call()* to get the total number of NFTs in existence
- *ExplorerToken.getLocation().call()* to get a specific NFT based on an index

- *ExplorerSupply.createToken().estimateGas()* to estimate the gas needed to execute the following operation

```

1
2 contract ExplorerToken is ERC721Enumerable, Ownable {
3     using Counters for Counters.Counter;
4     Counters.Counter private _tokenIds;
5
6     struct Location {
7         int24 latitude;
8         int24 longitude;
9         string name;
10    }
11
12    mapping(int24 => mapping(int24 => bool)) _coords;
13
14    mapping(uint256 => Location) _places;
15
16    constructor() ERC721("Explorer", "EXP") {}
17
18    function createToken(
19        int24 latitude,
20        int24 longitude,
21        string memory name
22    ) external onlyOwner returns (uint256) {
23        require(
24            _coords[latitude][longitude] == false,
25            "This location has already been registered!"
26        );
27
28        _tokenIds.increment();
29        uint256 locationId = _tokenIds.current();
30        _safeMint(this.owner(), locationId);
31        _places[locationId] = Location(latitude, longitude, name);
32        _coords[latitude][longitude] = true;
33        return locationId;
34    }
35
36    function getLocation(uint256 tokenId)
37        public
38        view
39        returns (Location memory)
40    {
41        _exists(tokenId);
42        return _places[tokenId];
43    }
44 }

```

Listing 1: ExplorerToken

```

1
2 contract ExplorerSupply is ERC1155, IERC721Receiver, Ownable {
3     address NFT;
4
5     constructor() ERC1155("") {
6         ExplorerToken _NFT = new ExplorerToken();
7         NFT = address(_NFT);
8     }
9
10    function ownedToken() external view returns (address _NFT) {
11        return NFT;
12    }

```

```

13
14     function onERC721Received(
15         address operator,
16         address from,
17         uint256 tokenId,
18         bytes calldata data
19     ) external override returns (bytes4) {
20         _mint(this.owner(), tokenId, 128, data);
21         return IERC721Receiver.onERC721Received.selector;
22     }
23
24     function createToken(
25         int24 latitude,
26         int24 longitude,
27         string memory name
28     ) public onlyOwner returns (uint256) {
29         ExplorerToken(NFT).createToken(latitude, longitude, name);
30         return 0;
31     }
32 }

```

Listing 2: ExplorerSupply