PD-10.0 Tokens





PD-10.1 ERC20 Tokens

PD-10.1 ERC20 Token Functions

Information functions (optional)

- name()
- symbol()
- decimals() → usually 18
- totalSupply()

Token interactions

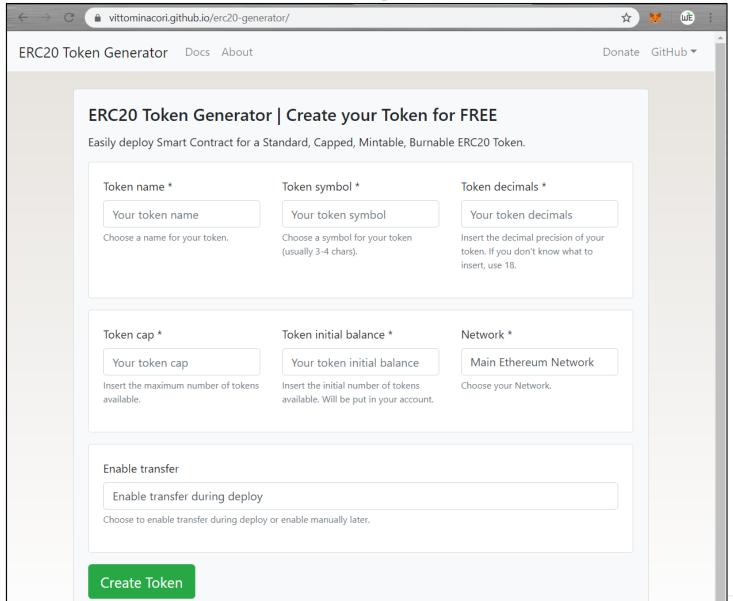
- balanceOf()
- Transfer()

Delegated token interactions

- transferFrom()
- Approve()
- allowance()



PD-10.1 ERC20 generator



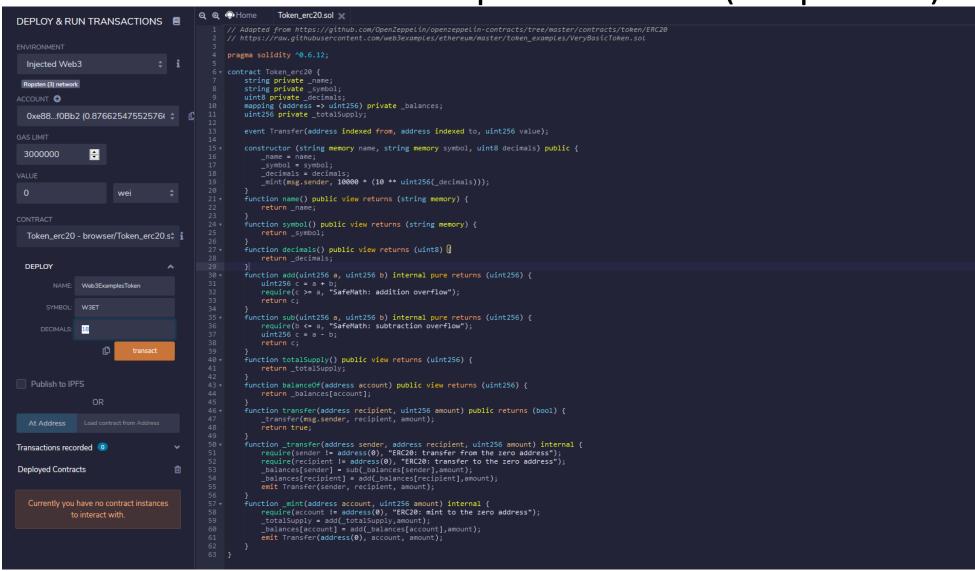
https://vittominacori.github.io/erc20-generator

http://web3examples.com/ethereum/demo/Create ERC20 via web.html

PD-10.1 Demo in Play

https://web3examples.com/ethereum/demo/Play ERC20.html

PD-10.1 Web3ExamplesToken (Ropsten)



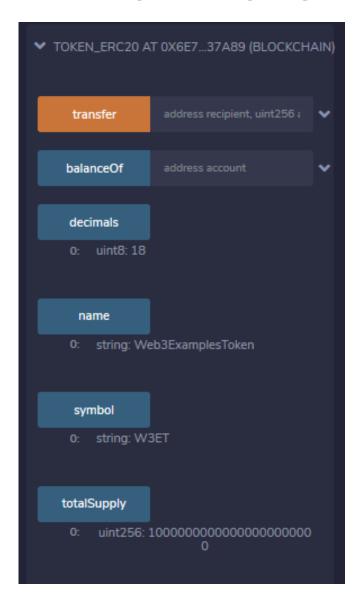
Parameters:

Web3ExamplesToken W3ET 18

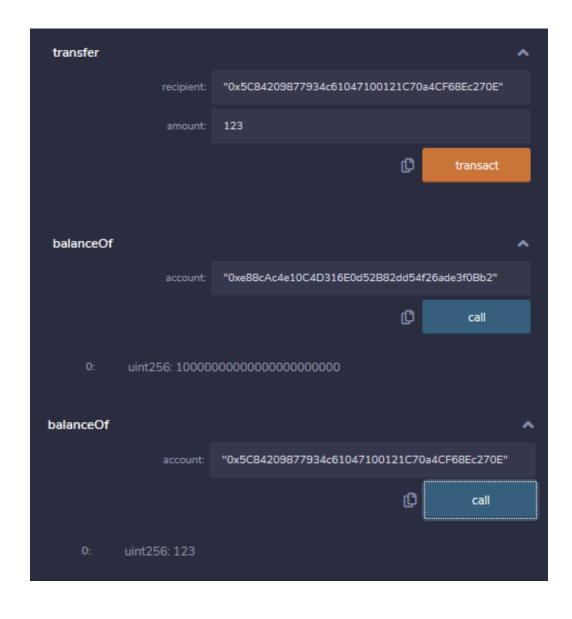
PD-10.1 Deployed Token



PD-10.1 Token info



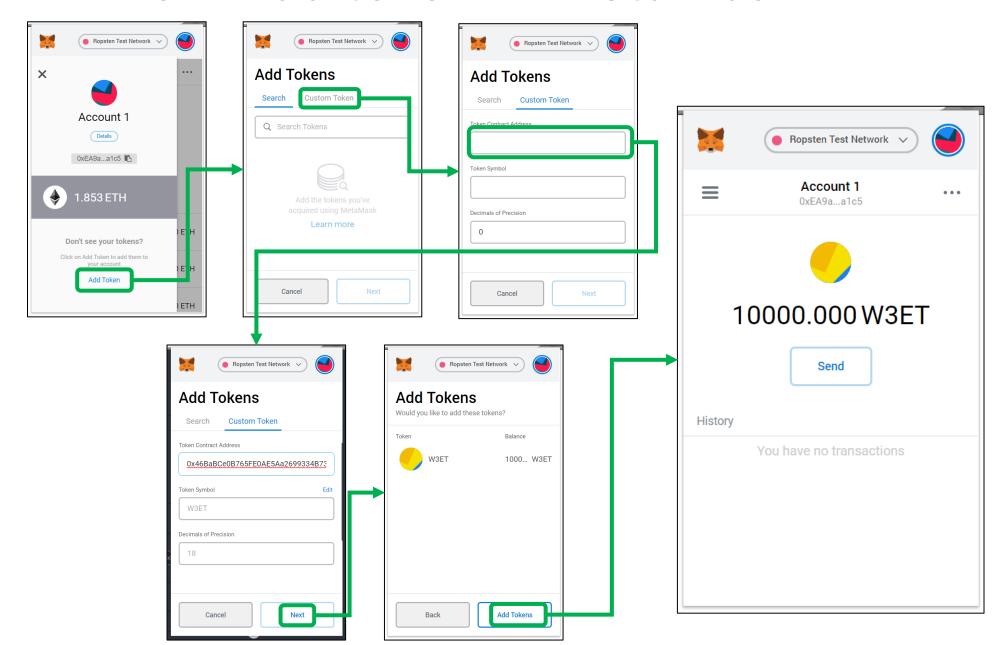
PD-10.1 BalanceOf & transfer



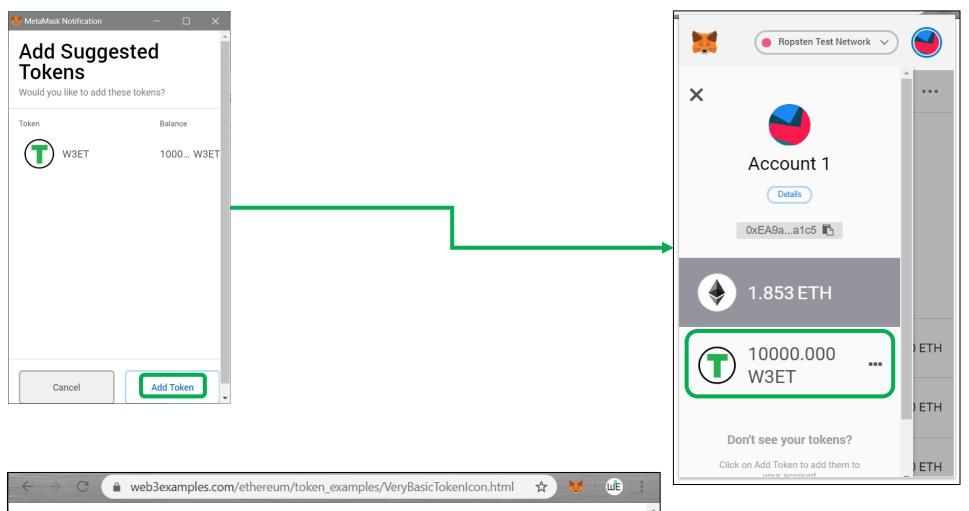
PD-10.1 VeryBasicToken.sol

```
function transfer(address recipient, uint256 amount) public returns (bool) {
    _transfer(msg.sender, recipient, amount);
    return true;
}
function _transfer(address sender, address recipient, uint256 amount) internal {
    require(sender != address(0), "ERC20: transfer from the zero address");
    require(recipient != address(0), "ERC20: transfer to the zero address");
    _balances[sender] = sub(_balances[sender],amount);
    _balances[recipient] = add(_balances[recipient],amount);
    emit Transfer(sender, recipient, amount);
}
```

PD-10.1 Add token in MetaMask



PD-10.1 Add Token Icon to MetaMask



VeryBasicToken Icon (Ropsten)

Adding icon for Web3ExamplesToken symbol W3ET decimals 18

Retrieving information from contract 0x46BaBCe0B765FE0AE5Aa2699334B734dbED6433D

Image https://web3examples.com/ethereum/token examples/VeryBasicTokenIcon.png

Version of web3.js: 1.2.4

https://github.com/ethereum/EIPs/blob/master/EIPS/eip-747.md

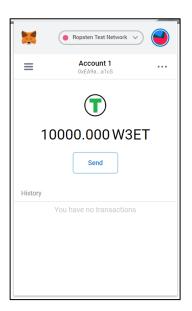
https://web3examples.com/ethereum/token examples/VeryBasicTokenIcon.html

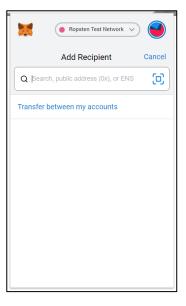
https://github.com/web3examples/ethereum/blob/master/token_examples/VeryBasicTokenIcon.html

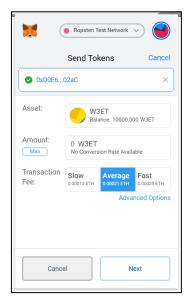
PD-10.1 Source to add Token Icon to MetaMask

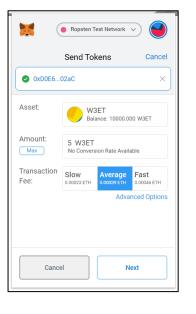
```
var VeryBasicTokenAddress="0x31a289430c79a38Ae290B9789DE4992710d796Ec";
var VeryBasicTokenContract=new web3.eth.Contract(VeryBasisTokenABI, VeryBasicTokenAddress);
log(`Retrieving information from contract ${VeryBasicTokenAddress}`);
const name
              = await VeryBasicTokenContract.methods.name()
    .call({from: acts[0]}).catch(console.log);
const symbol = await VeryBasicTokenContract.methods.symbol()
    .call({from: acts[0]}).catch(console.log);
const decimals = await VeryBasicTokenContract.methods.decimals()
    .call({from: acts[0]}).catch(console.log);
const url = new URL("VeryBasicTokenIcon.png", window.location.href);
log(`Adding icon for ${name} symbol ${symbol} decimals ${decimals}`);
log(`Image ${url.href}`);
const params={type: 'ERC20', "options": {
    "address": VeryBasicTokenAddress,
    "decimals": decimals,
    "symbol": symbol,
    "decimals": decimals,
   "image": url.href
window.web3.currentProvider.sendAsync({
   method: 'metamask watchAsset',
   params: params,
   id: Math.round(Math.random() * 100000),
  (err) => console.log(err) );
```

PD-10.1 Transfer tokens

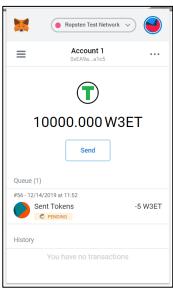


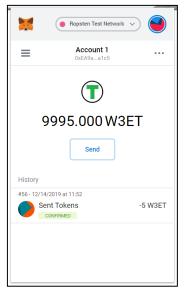


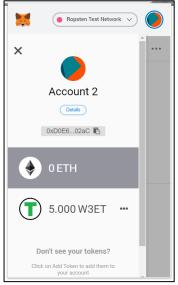








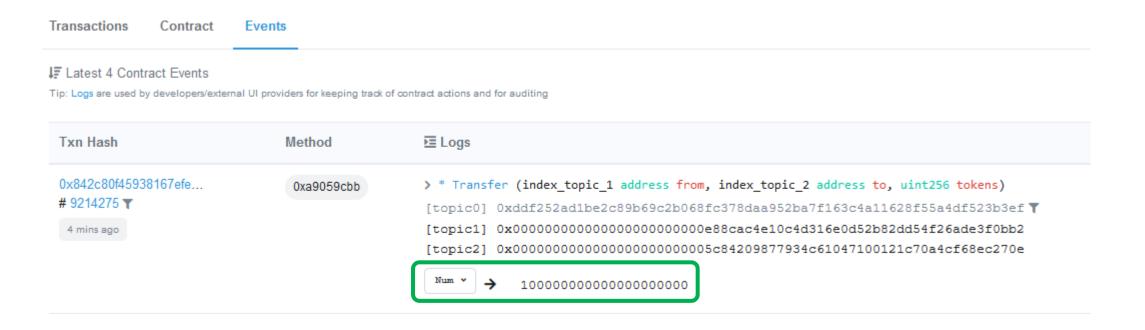




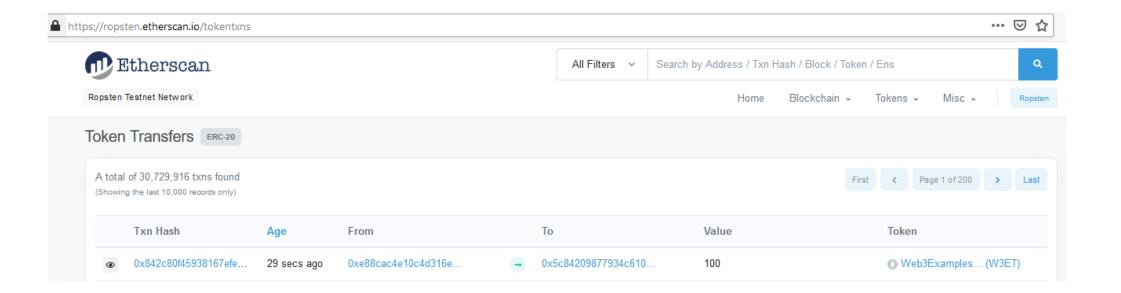
PD-10.1 Etherscan - logs



PD-10.1 After verification



PD-10.1 Recognized as a token transaction



PD-10.1 Etherscan – token info

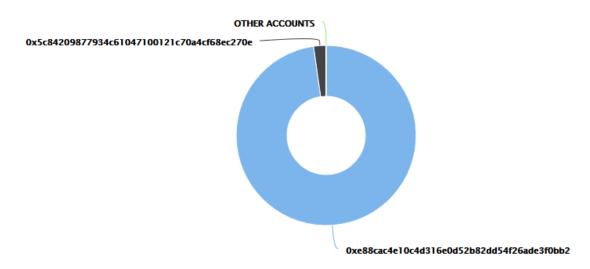


PD-10.1 Etherscan — token info

↑ The top 100 holders collectively own 100.00% (10,000.00 Tokens) of Web3ExamplesToken

Web3ExamplesToken Top 100 Token Holders

Source: Etherscan.io



(A total of 10,000.00 tokens held by the top 100 accounts from the total supply of 10,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0xe88cac4e10c4d316e0d52b82dd54f26ade3f0bb2	9,776.9999999999999977	97.7700%
2	0x5c84209877934c61047100121c70a4cf68ec270e	223.0000000000000123	2.2300%

https://ropsten.etherscan.io/token/tokenholderchart/0x6e717970b902e29208d2b6fcfca13594b3c37a89

PD-10.1 Opnzeppelin contracts

>npm install @openzeppelin/contracts

+ @openzeppelin/contracts@2.4.0 added 1791 packages from 856 contributors, removed 2 packages, updated 2 packages and audited 1036357 packages in 93.908s

PD-10.1 Truffle - OpenZeppelin - ERC20

https://github.com/web3examples/ethereum/blob/master/token_examples/ERC20TruffleOpenZeppelin/contracts/Token_erc20.sol

PD-10.1 Included libraries

```
> tree /f
    truffle-config.js
   -build
       -contracts
            Context.json
            ERC20.json
            ERC20Detailed.json
            IERC20.json
            Migrations.json
            SafeMath.json
            Token erc20.json
   -contracts
        Migrations.sol
        Token erc20.sol
   -migrations
        1 initial migration.js
        2 token erc20.js
   -test
```

PD-10.1 SafeMath

```
library SafeMath {
     * @dev Returns the addition of two unsigned integers, reverting on
    * overflow.
    * Counterpart to Solidity's `+` operator.
    * Requirements:
     * - Addition cannot overflow.
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
       uint256 c = a + b;
       require(c >= a, "SafeMath: addition overflow");
       return c;
```

PD-10.2 ERC721 Tokens

Non fungible tokens

PD-10.2 ERC721 Token Functions

Information functions (optional)

- name()
- symbol()

Token interactions

- ownerOf()
- transferFrom()

Safe token interactions

safeTransferFrom()

Delegated token interactions

- Approve()
- setApprovalForAll()
- getApproved()
- isApprovedForAll()
- Receive NFT's
 - onERC721Received()
- Verification
 - supportsInterface()



PD-10.2 ERC721 demo's

https://web3examples.com/ethereum/demo/Play Deploy contract ERC721.html

https://web3examples.com/ethereum/demo/Play See ERC721 token in Metamask.html

https://web3examples.com/ethereum/demo/Play Mint one ERC721 token.html

PD-10.2 VeryBasicNFT.sol

```
function settleTransfer(address from, address to, uint256 tokenId) internal
   removeToken( from, tokenId);
   addToken( to, tokenId);
   emit Transfer( from, to, tokenId);
function addToken(address to, uint256 tokenId) internal {
   allTokens.push( tokenId);
   allTokensIndex[ tokenId] = allTokens.length-1;
   ownerOfToken[ tokenId] = to;
   ownedTokens[ to].push( tokenId);
   ownedTokensIndex[ tokenId] = ownedTokens[ to].length-1;
function removeToken(address from, uint256 tokenId) internal {
   uint256 allIndex = allTokensIndex[ tokenId];
   uint256 allTokensLength = allTokens.length;
   allTokens[allIndex] = allTokens[allTokensLength - 1];
   allTokensIndex[allTokens[allTokensLength-1]] = allIndex;
   delete allTokens[allTokensLength-1];
   allTokens.length -= 1;
   uint256 ownerIndex = ownedTokensIndex[ tokenId];
   uint256 ownerLength = ownedTokens[ from].length;
   ownedTokens[ from][ownerIndex] = ownedTokens[ from][ownerLength-1];
   ownedTokensIndex[ownedTokens[ from][ownerLength-1]] = ownerIndex;
   delete ownedTokens[ from][ownerLength-1];
   ownedTokens[ from].length -= 1;
   delete ownerOfToken[ tokenId];
```

PD-10.2 createToken

```
uint256 public counter = 10;

function createToken(address _minter) public {
    require(msg.sender == admin);
    addToken(_minter, counter);
    emit Transfer(address(0), _minter, counter);
    counter += 1; // every new token gets a new ID
}
```

PD-10.2 Deploy via Play (On Rinkeby)

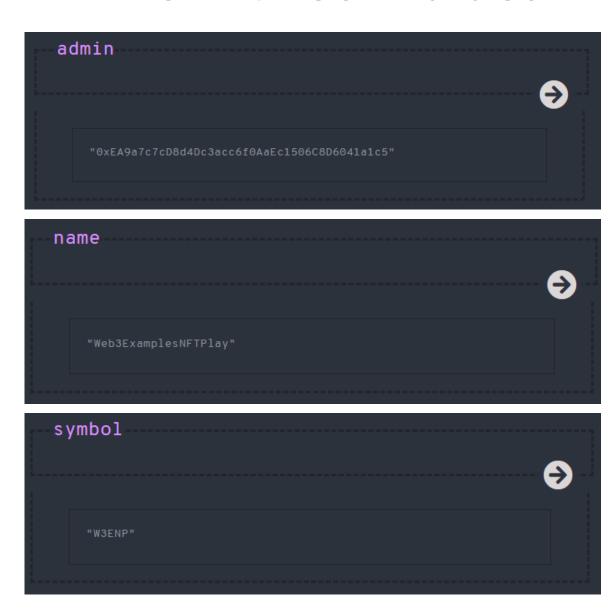




Web3ExamplesNFTPlay W3ENP

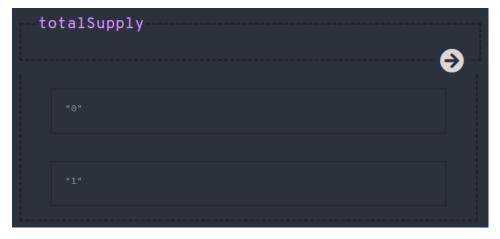
0x2e9cc4cd27640e820f272f0272a09cae78aa0fe2

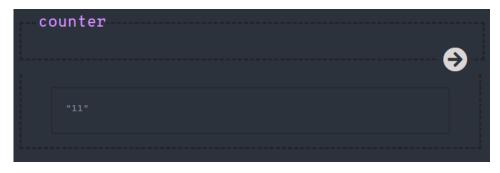
PD-10.2 Check values



PD-10.2 CreateToken

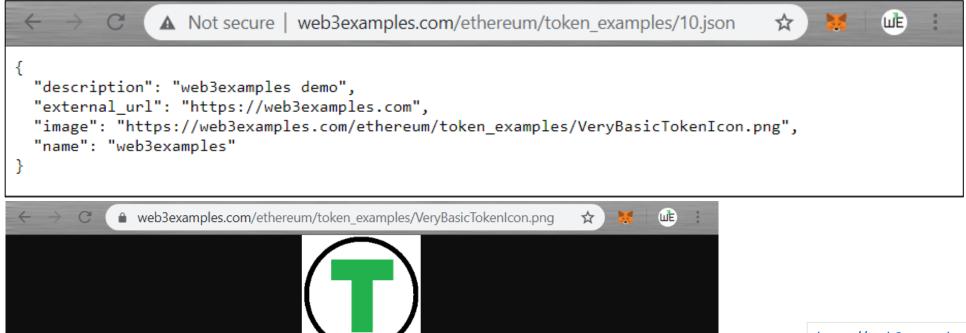






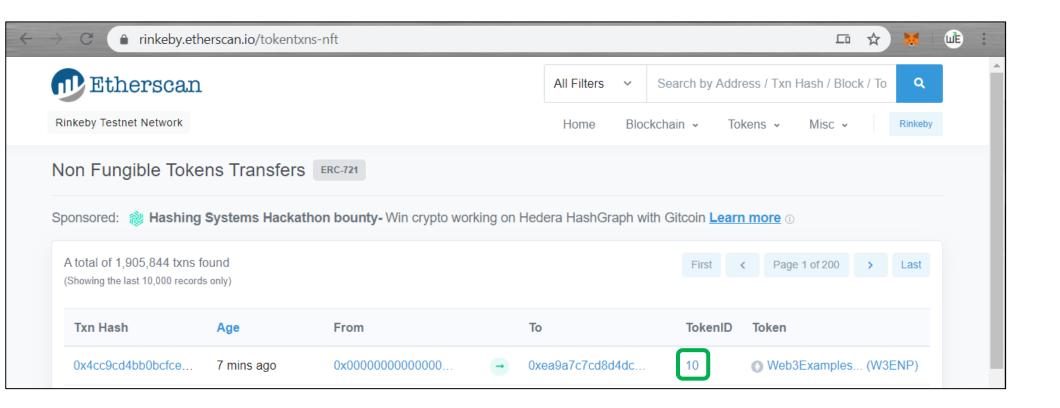
PD-10.2 setToken URI



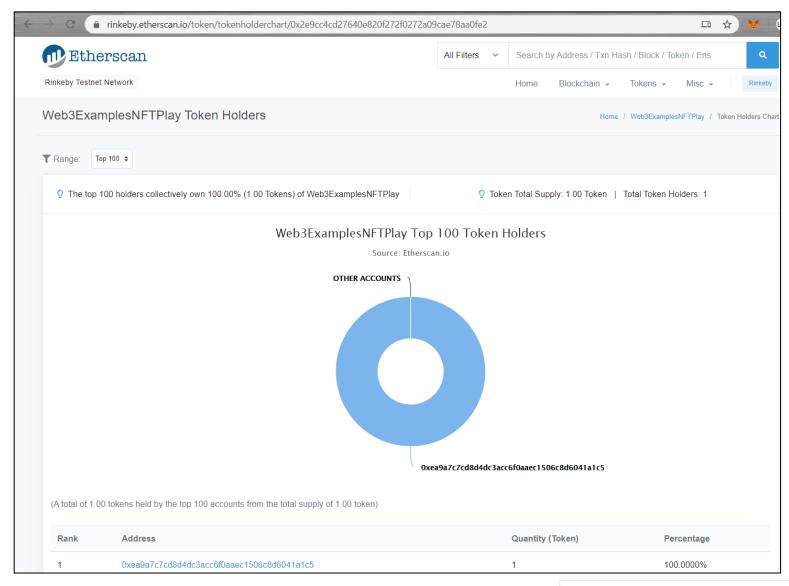


https://web3examples.com/ethereum/token_examples/10.json

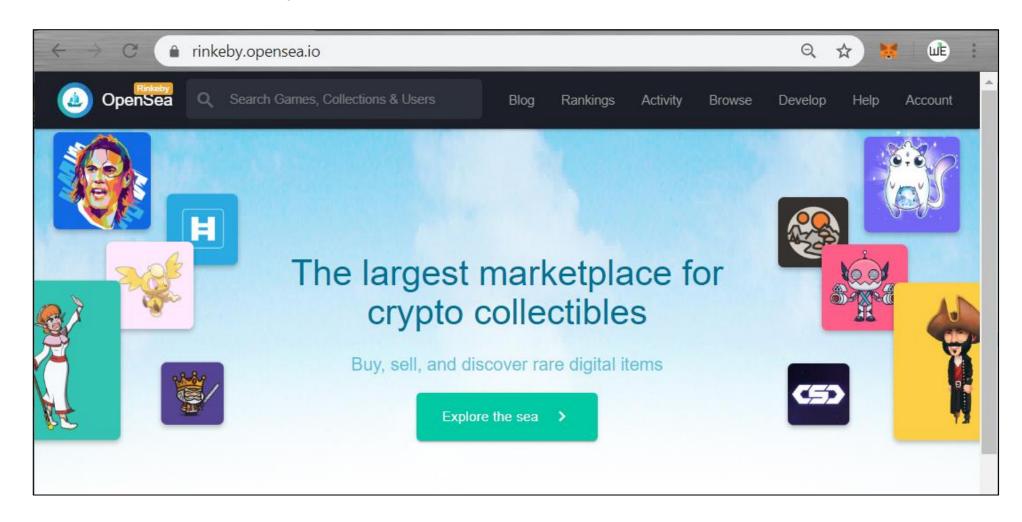
PD-10.2 Etherscan (after verification of source)



PD-10.2 Etherscan Token Holders



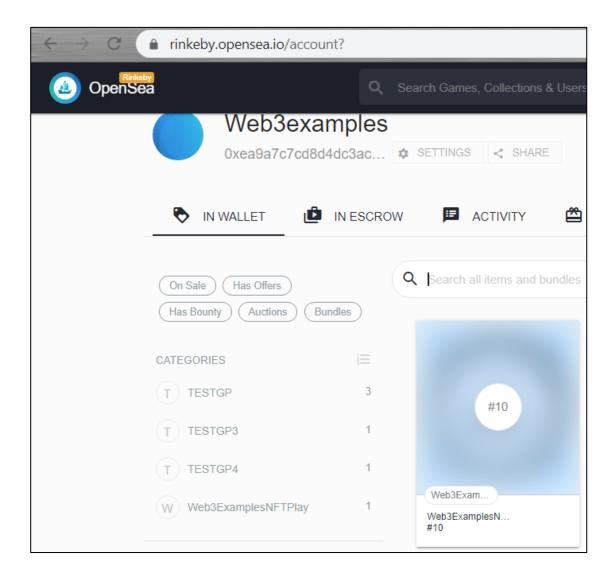
PD-10.2 OpenSea

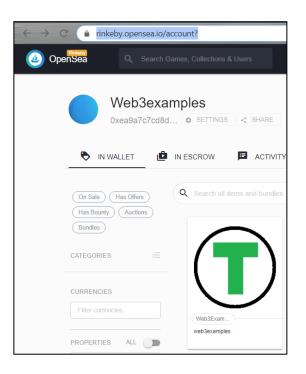


https://opensea.io

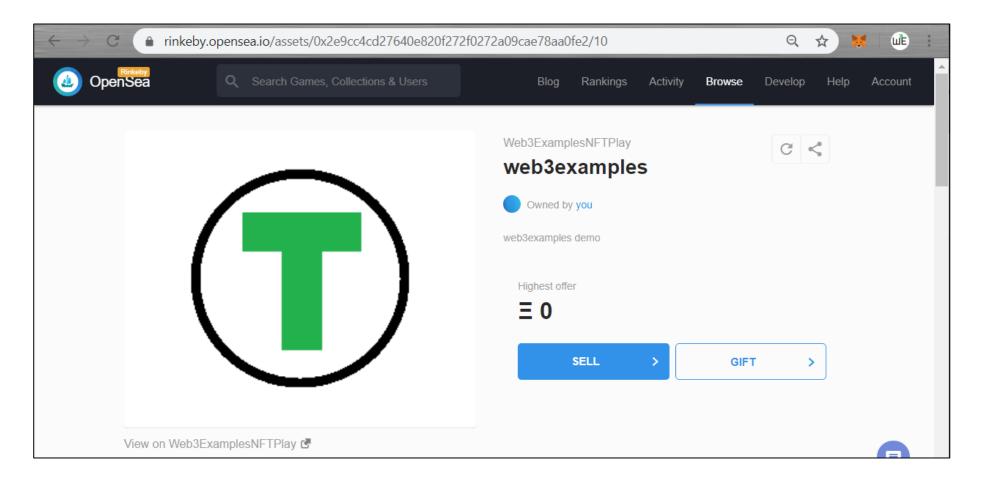
https://rinkeby.opensea.io/

PD-10.2 OpenSea





PD-10.2 OpenSea asset



 $\underline{https://rinkeby.opensea.io/assets/0x2e9cc4cd27640e820f272f0272a09cae78aa0fe2/10assets/0x2e9cc4cd27640e820f272f02640e820f272f02640e820f2640e80f2660e80f2660e80f2660e80f2660e80f2660e80f2660e80f2600e80f2600e80f26$

https://web3examples.com/ethereum/demo/Find ERC721 token in Opensea.html

PD-10.2 Datastructure ERC721

AllTokens (array)

1 Token 1: 0x123

2 Token 2: 0x456

3 Token 3: 0x789

AllTokensIndex	
Token 1: 0x123	1
Token 2: 0x456	2
Token 3: 0x789	3

ownedTokens (mapping & array)

Account 1: 0xabc	1	Token 1: 0x123
	2	Token 3: 0x789
	3	
Account 2: 0xdef	1	Token 2: 0x456
	2	

ownerOfToken (mapping)

Token 1: 0x123 Account 1: 0xabc

Token 2: 0x456 Account 2: 0xdef

Token 3: 0x789 Account 1: 0xabc

ownedTokensIndex

Token 1: 0x123	1
Token 2: 0x456	1
Token 3: 0x789	2

tokenURIs (mapping)

Token 1: 0x123 https://..../10.json

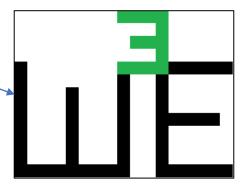
Token 2: 0x456 https://..../11.json

Token 3: 0x789 https://..../12.json

PD-10.2 JSON Structure

https://..../10.json

```
"description": "web3examples demo",
  "external_url": "https://web3examples.com",
  "image": "https://web3examples.com/logo.png",
  "name": "web3examples"
}
```



PD-10.2 ERC721 Metadata JSON Schema

```
"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"
```

PD-10.2 OpenSea MetaData

image	This is the URL to the image of the item. Can be just about any type of image (including SVGs, which will be cached into PNGs by OpenSea), and can be IPFS URLs or paths.
image_data	Raw SVG image data, if you want to generate images on the fly (not recommended). Only use this if you're not including the <code>image</code> parameter.
external_url	This is the URL that will appear below the asset's image on OpenSea and will allow users to leave OpenSea and view the item on your site.
description	A human readable description of the item. Markdown is supported.
name	Name of the item.
attributes	These are the attributes for the item, which will show up on the OpenSea page for the item. (see below)
background_color	Background color of the item on OpenSea. Must be a six-character hexadecimal <i>without</i> a prepended #.
animation_url	A URL to an animated image of the item. GLTF, GLB, and WEBM are supported.
youtube_url	A URL to a YouTube video.

https://docs.opensea.io/docs/metadata-standards

PD-10.2 ERC-165

Creates a standard method to publish and detect what interfaces a smart contract implements.

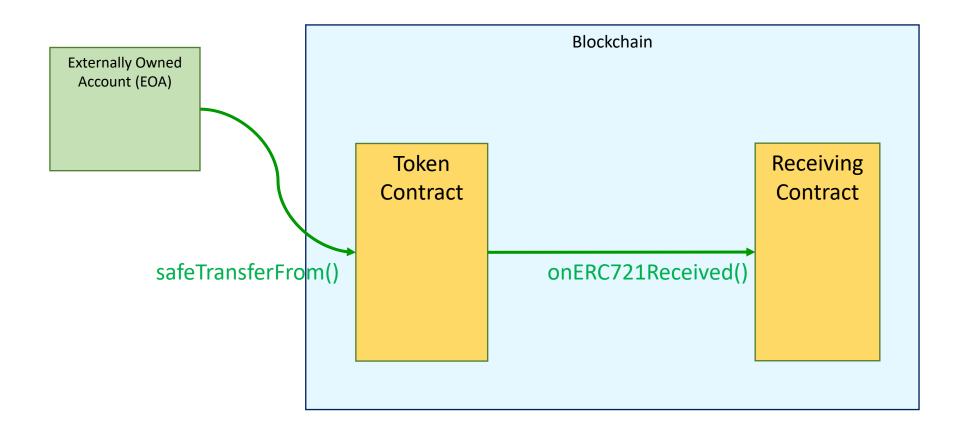
```
function supportsInterface(bytes4
interfaceID) constant returns (bool) {
   If (interfaceID == i0) return false;
   If (interfaceID == i1) return true;
   If (interfaceID == i2) return true;
   If (interfaceID == i3) return true;
   return false;
}
```

```
i0=0xffffffff
                                 function supportsInterface(..) ..
i1=this.supportsInterf
ace.selector
(0x01ffc9a7)
                                 function f1(..) ...
i2=this.f1.selector ^
                                 0x20202020
this.f2.selector;
                                 function f2(..) ...
0x21212121
                                 0x01010101
                                 function f3(..) ...
i3=this.f3.selector ^
                                 0x00030000
this.f4.selector ^
                                 function f4(..) ...
this.f5.selector;
                                 0x00000400
0x00030405
                                 function f5(..) ...
```

0x00000005

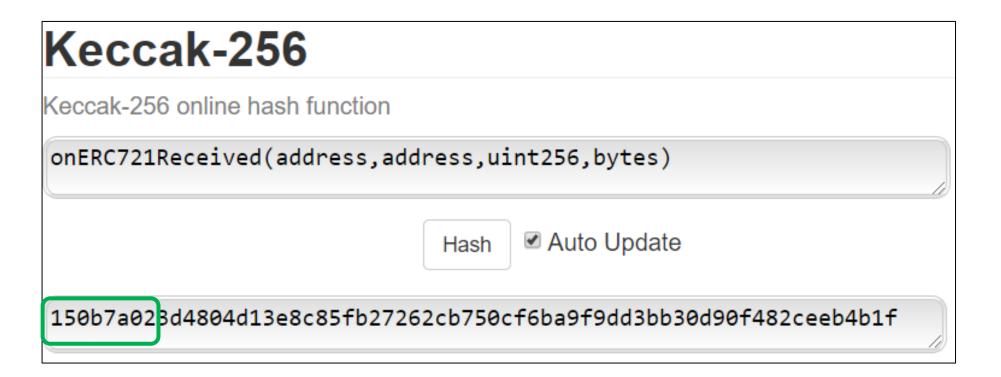
https://github.com/ethereum/EIPs/blob/master/EIPS/eip-165.md

PD-10.2 on ERC721Received



PD-10.2 on ERC721Received signature

bytes4(keccak256("onERC721Received(address, address, uint256, bytes)"));
bytes4 internal constant ONERC721RECEIVED_FUNCTION_SIGNATURE = 0x150b7a02;



https://www.4byte.directory/

PD-10.2 ERC721TokenReceiver

```
bytes4 internal constant ONERC721RECEIVED_FUNCTION_SIGNATURE = 0x150b7a02;

function onERC721Received(address _operator, address _from, uint256
   _tokenId, bytes memory _data) public returns(bytes4) {
        receivedOperator = _operator;
        receivedFrom = _from;
        receivedTokenId = _tokenId;
        receivedData = _data;
        return ONERC721RECEIVED_FUNCTION_SIGNATURE;
    }
```

PD-10.2 safeTransferFrom

```
bytes4 internal constant ONERC721RECEIVED FUNCTION SIGNATURE = 0x150b7a02;
function safeTransferFrom(address from, address to, uint256 tokenId,
bytes memory data) public payable
    tokenExists( tokenId)
    allowedToTransfer( from, _to, _tokenId) {
        settleTransfer( from, to, tokenId);
        uint256 size;
        assembly { size := extcodesize( to)
        if (size > 0) {
            require (EIP721 ( to).onERC721Received (
               msg.sender, from, tokenId, data)
               == ONERC721RECEIVED FUNCTION SIGNATURE);
```

PD-10.2 ERC721 via Truffle

https://github.com/web3examples/ethereum/blob/master/token_examples/ERC721TruffleOpenZeppelin/contracts/Token_erc721.sol

PD-10.2 Included libraries

```
> tree /f
    truffle-config.js
   -build
      --contracts
            Address.json
            Context.json
            Counters.json
            ERC165.json
            ERC721.json
            ERC721Enumerable.json
            ERC721Full.json
            ERC721Metadata.json
            ERC721Mintable.json
            IERC165.json
            IERC721.json
            IERC721Enumerable.json
            IERC721Metadata.json
            IERC721Receiver.json
            Migrations.json
            MinterRole.json
            Roles.json
            SafeMath.json
            Token erc721.json
   -contracts
        Migrations.sol
        Token erc721.sol
   -migrations
        1 initial migration.js
        2 token erc721.js
   -test
```