*ERC20/ERC721*の発行

株式会社Neo Breakthrough

山科 優希

使用するも

- *Google Chrome*
- *Metamask*（インストール済み）
- *Remix*
  →*Remix*は*Web*ブラウザ上で*Solidity*言語によるコントラクトの作成・コンパイル・
    実行を行える開発環境
- ~~*GoerliETH*~~ *or Mumbai MATIC*
  →Testnetトークン（~~Goerli：Ethereum Mumbai~~：Matic Mainnet）
- *OpenZeppelin*
  →*Solidity*言語によるスマートコントラクトのオープンフレームワーク
- *OpenZeppelin Contract Wizard*
  →スマートコントラクトの実装がGUI画面にて可能であり、Remixへの連携アリ

Goerli

Testnet

Goerli (long-term support)

Note: *the Goerli testnet is deprecated ↗ and will be replaced by Holesovice ↗ in 2023. Please consider migrating your applications to Sepolia.*

Goerli is testnet for testing of validating and staking. The Goerli network is open for users wanting to run a testnet validator. Stakers wanting to test protocol upgrades before they are deployed to mainnet should therefore use Goerli.

- Open validator set, stakers can test network upgrades
- Large state, useful for testing complex smart contract interactions
- Longer to sync and requires more storage to run a node

"*Goerli*テストネットは非推奨で、*2023*年に*Holesovice*に置き換わる予定"

"*Goerli*ネットワークは、テストネットバリデータを実行したいユーザーのために開かれている"

"オープンなバリデータセットで、ステイカーはネットワークのアップグレードをテストすることができる"

Sepolia

Testnet

Sepolia

Sepolia is the recommended default testnet for application development. The Sepolia network uses a permissioned validator set. It's fairly new, meaning its state and history are both quite small. This means the network is quick to sync to and that running a node on it requires less storage. This is useful for users who want to quickly spin up a node and interact with the network directly.

- Closed validator set, controlled by client & testing teams

- New testnet, less applications deployed than other testnets

- Fast to sync and running a node requires minimal disk space

*"Sepolia*は、アプリケーション開発のための推奨されるデフォルトのテストネット"

"許可されたバリデータを使用している"

"新しいテストネットであり、他のテストネットに比べてアプリケーションのデプロイが少ない"

*Goerli*ではなく*Polygon Mumbai*を選択

- *Ethereum*も*Polygon*も*solidity*でスマコン書ける
- *Polygon*の方が手数料安い
- 資料作成時（3月17日）においてGoerli FaucetでClaimできない（なぜ）
  →Faucetは『蛇口』を意味しており、Faucetを利用することで
    *Testnet Token*を獲得できる

*ERC20*発行 事前準備

1.OpenZeppelin Contract Wizard

2.Polygon Faucet

3.Mumbai Polygonscan

*ERC20*を発行する

Name：トークン名

ex)Ethereum

Symbol：シンボル

ex)ETH

Premint：初期発行枚数

DEPLOY & RUN TRANSACTIONS ✓ ›

ENVIRONMENT 🔌

Injected Provider - MetaMask ⇅ ⓘ

Custom (80001) network

ACCOUNT ⊕

0x3C4...9f272 (0.19705524ⁱ ⇅ ⧉ ✎

GAS LIMIT

3000000

VALUE

0   Wei ⇅

CONTRACT (Compiled by Remix)

NeoToken - contract-405440dcdf.sol ⇅

Deploy

☐ Publish to IPFS

OR

At Address   Load contract from Address

Transactions recorded 0 ⓘ   ›

Deployed Contracts

Currently you have no contract
instances to interact with.

```
1   // SPDX-License-Identifier: MIT
2   pragma solidity ^0.8.9;
3
4   import "@openzeppelin/contracts@4.8.2/token/ERC20/ERC20.sol";
5
6   contract NeoToken is ERC20 {
7       constructor() ERC20("NeoToken", "NEO") {
8           _mint(msg.sender, 123456789 * 10 ** decimals());
9       }
10  }
11
```

▶ 🔍 🔍 🏠 Home $ contract-405440dcdf.sol ✕

⤓ 🚫 0 ☐ listen on all transactions 🔍 Search with transaction hash or address

creation of NeoToken pending...

✓ [vm] from: 0x5B3...eddC4 to: NeoToken.(constructor) value: 0 wei data: 0x608...20033 logs: 1 hash: 0x0b5...0074a

Debug ⌄

›

🦊 ⦿ Polygon Mumbai Testnet ⌄

● Connected   **Account 2**   ⋮
                0x3C4...f272 ⧉

0.1971 MATIC

$0.23 USD

⤓   ↗   ⇄
Buy   Send   Swap

Assets   Activity

📈 Portfolio site

0.1971 MATIC   ›
$0.23 USD

Don't see your token?

DEPLOY & RUN TRANSACTIONS ✔ ›

contract-405440dcdf.sol ✕

```
1  // SPDX-License-Identifier: MIT
2  pragma solidity ^0.8.9;
3
4  import "@openzeppelin/contracts@4.8.2/token/ERC20/ERC20.sol";
5
6  contract NeoToken is ERC20 {
7      constructor() ERC20("NeoToken", "NEO") {
8          _mint(msg.sender, 123456789 * 10 ** decimals());
```

ENVIRONMENT 🔌

Injected Provider - MetaMask
Custom (80001) network

ACCOUNT ⊕
0x3C4...9f272 (0.19116564§

GAS LIMIT
3000000

VALUE
0   Wei

CONTRACT (Compiled by Remix)
NeoToken - contract-405440dcdf.sol

Deploy

☐ Publish to IPFS

OR

At Address   Load contract from Address

Transactions recorded ② ⓘ   ›

Deployed Contracts   🗑

› NEOTOKEN AT 0X8B6...F5B69 (BLOC

⌄ ⊘ 0 ☐ listen on all transactions   🔍 Search with transaction hash or address

✔ [block:33215482 txIndex:0] from: 0x3C4...9f272 to: NeoToken.(constructor) value: 0 wei data: 0x608...20033 logs: 1 hash: 0x5b4...47b2f   **Debug** ⌃

status   true Transaction mined and execution succeed

transaction hash   0xf8e4c928c29e16fd4d4620ae4be50d8e19bc2308e2a9c385e2e9f07b635a0a86 ⎘

from   0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272 ⎘

to   NeoToken.(constructor) ⎘

gas   1177920 gas ⎘

transaction cost   1177920 gas ⎘

input   0x608...20033 ⎘

decoded input   {} ⎘

decoded output   - ⎘

logs   [
                                {
                                  "from": "0x8B6cB258429b5DBA2bAF81288dB46031715F5B69",
                                  "topic": "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
                                  "event": "Transfer",
                                  "args": {
                                    "0": "0x0000000000000000000000000000000000000000",
                                    "1": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
                                    "2": "123456789000000000000000000",
                                    "from": "0x0000000000000000000000000000000000000000",
                                    "to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
                                    "value": "123456789000000000000000000"
                                  }
                                }
                              ] ⎘ ⎘

>

[block:33215482 txIndex:0] **from:** 0x3C4...9f272 **to:** NeoToken.(constructor) **value:** 0 wei **data:** 0x608...20033 **logs:** 1 **hash:** 0x5b4...47b2f

`Debug`

status	true Transaction mined and execution succeed
transaction hash	0xf8e4c928c29e16fd4d4620ae4be50d8e19bc2308e2a9c385e2e9f07b635a0a86
from	0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272
to	NeoToken.(constructor)
gas	1177920 gas
transaction cost	1177920 gas
input	0x608...20033
decoded input	{}
decoded output	-
logs	

```
[
    {
        "from": "0x8B6cB258429b5DBA2bAF81288dB46031715F5B69",
        "topic": "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
        "event": "Transfer",
        "args": {
            "0": "0x0000000000000000000000000000000000000000",
            "1": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
            "2": "123456789000000000000000000",
            "from": "0x0000000000000000000000000000000000000000",
            "to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
            "value": "123456789000000000000000000"
        }
    }
]
```

val	0 wei

発行したERC20をMetamaskに表示

METAMASK

Polygon Mumbai Testnet ⌄

Import tokens ✕

Custom token

ℹ Token ....tion is not available on t......ork yet.
Please import token manually and make sure you tru....
Learn about scams and security risks.

Token contract address

Token symbol

Token decimal

0

Add custom token

METAMASK

Polygon Mumbai Testnet ⌄

Import tokens

Would you like to import these tokens?

Token	Balance
NEO	123456789 NEO

Back

Import tokens

*ERC20*発行 終

*ERC721*発行 事前準備

Pinata（*IPFS*と通信を行う*Public Gateway*サービスの一種）
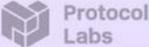
*IPFS*の復習

- *IPFS*はコンテンツ指向型のハイパーメディア分散プロトコル
- *IPFS*は*HTTP*をベースとした既存のネットワークとは独立したネットワーク
  →既存のブラウザからアクセスするにはIPFSに橋渡ししてくれる存在が必要
  →IPFS Gateway
- *IPFS Gateway*の中でも任意ユーザーに常時公開されている*IPFS Public Gateway*（https://ipfs.io/ipfsなど）を利用する必要がある
- *https://ipfs.io/ipfs/*〜〜〜の『〜〜〜』部にコンテンツ（*Content*）の*ID*（画像等のコンテンツのハッシュ値）を入れる必要がある（*CID*）
  →逆に言えば、上記のコンテンツIDを知っているものであれば閲覧可能
- *P2P*ファイル共有システムによって耐障害性、耐検閲性、耐改ざん性がある
- 詳細な仕組みについては添付リンク参照
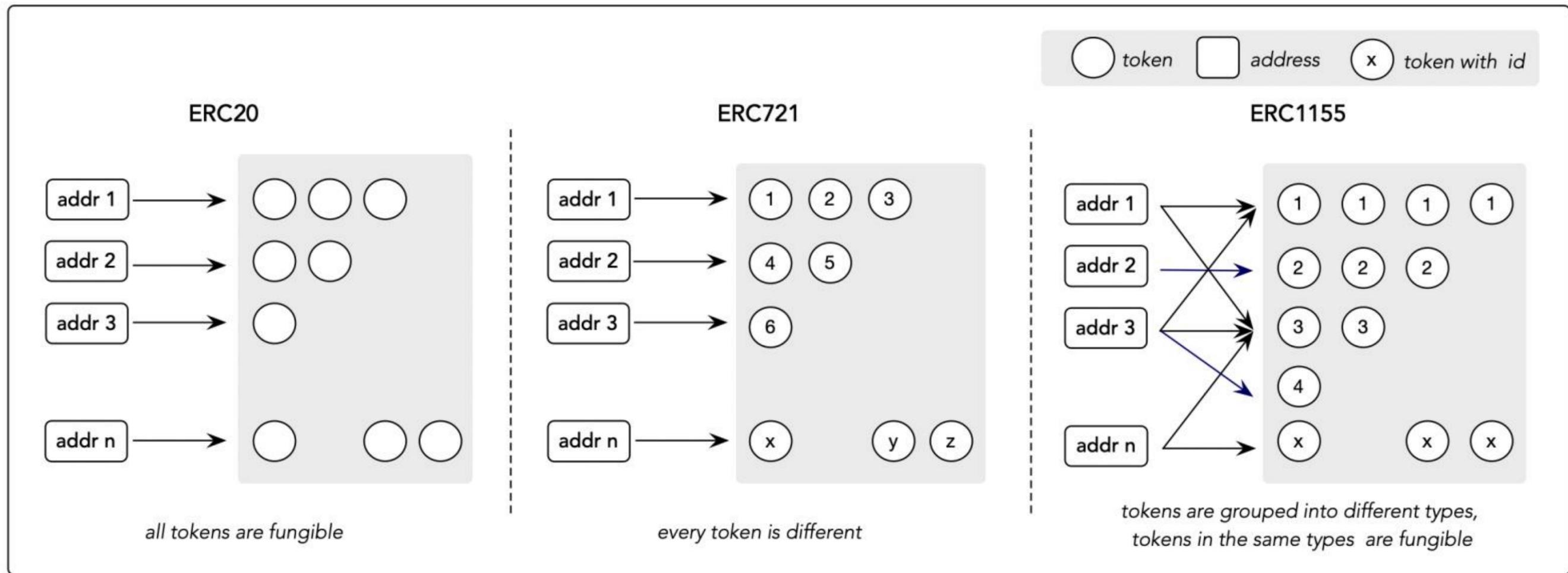
Fig. 2: NFT-related Token Standards
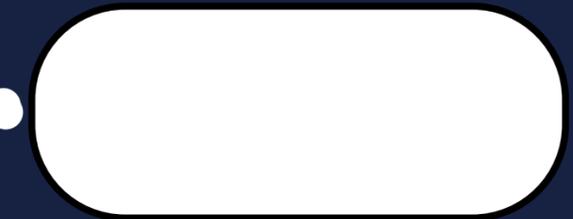
*ERC721*を発行する

画像データの準備

Welcome
to Pinata!

Pinata is the leading media management company for creators and developers building the future of web3.

Log in   ## Sign up

Email*

Which title describes you the best?

Builder   Creator

Next

コントラクト

OpenZeppelin | contracts

Solidity Wizard   Cairo Wizard

Forum Docs GitHub Twitter

ERC20 **ERC721** ERC1155 Governor Custom

Copy to Clipboard   Open in Remix   Download

SETTINGS

Name | Symbol
MyToken | MTK

Base URI
https://...

FEATURES

☐ Mintable
 └☐ Auto Increment Ids
☐ Burnable
☐ Pausable
☐ Votes
☐ Enumerable
☐ URI Storage

ACCESS CONTROL ☐

○ Ownable
○ Roles

UPGRADEABILITY ☐

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.9;

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

contract MyToken is ERC721 {
    constructor() ERC721("MyToken", "MTK") {}
}
```

COMPILER

0.8.18+commit.87f61d96

Include nightly builds

Auto compile

Hide warnings

Advanced Configurations

⟳ Compile contract-4c6e1364..

Compile and Run script

CONTRACT

StakeToken (contract-4c6e136413.sol

Publish on Ipfs **IPFS**

Publish on Swarm

Compilation Details

ABI   Bytecode

```solidity
1   // SPDX-License-Identifier: MIT
2   pragma solidity ^0.8.9;
3
4   import "@openzeppelin/contracts@4.8.2/token/ERC721/ERC721.sol";
5   import "@openzeppelin/contracts@4.8.2/access/Ownable.sol";
6
7   contract StakeToken is ERC721, Ownable {
8       constructor() ERC721("StakeToken", "STT") {}
9
10      function _baseURI() internal pure override returns (string memory) {
11          return "https://gateway.pinata.cloud/ipfs/QmQcra56Qzg4BqoA3wJ2fTcHvDuzUR2FUEZcwnV4ADSi2K";
12      }
13
14      function safeMint(address to, uint256 tokenId) public onlyOwner {
15          _safeMint(to, tokenId);
16      }
17  }
18
```

Home   contract-4c6e136413.sol

0   listen on all transactions   Search with transaction hash or address

web3 version 1.5.2
ethers.js
remix

Type the library name to see available commands.

>

[block:33217583 txIndex:2] from: 0x3C4...9f272 to: StakeToken.(constructor) value: 0 wei data: 0x608...20033 logs: 1 hash: 0xcca...10f03

status	true Transaction mined and execution succeed
transaction hash	0x45ea3a249c514896909eb1716c0957107a9bcc9484efc9681bbb95e617225c5a
from	0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272
to	StakeToken.(constructor)
gas	2373699 gas
transaction cost	2373699 gas
input	0x608...20033
decoded input	{}
decoded output	–
logs	
val	0 wei

```
[
    {
        "from": "0x367e52b9cBE82d9dCbd6C4078D319e32080fB803",
        "topic": "0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0",
        "event": "OwnershipTransferred",
        "args": {
            "0": "0x0000000000000000000000000000000000000000",
            "1": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
            "previousOwner": "0x0000000000000000000000000000000000000000",
            "newOwner": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272"
        }
    }
]
```

token id

address

NFT発行
＝所有権の割り当
て

CA

NEW!!

1

2

3

4

EOA-1

EOA-2

EOA-3

token id

address

NEW!!

NFT発行
＝所有権の割り当
て

1

EOA-1

EOA-2

CA

EOA-3

✅ **[block:33218715 txIndex:2]** **from:** 0x3C4...9f272 **to:** StakeToken.safeMint(address,uint256) 0xa37...38446 **value:** 0 wei **data:** 0xa14...00000 **logs:** 1
hash: 0x2a1...2ea06

status	true Transaction mined and execution succeed
transaction hash	0xc540d4af547b6f15e0a3ff5fe4613d0149cf35a7b5c8c9b4620bca-a7668c0c7 📋
from	0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272 📋
to	StakeToken.safeMint(address,uint256) 0xa373777C97B996A00E62497d85C781a2BEa38446 📋
gas	72139 gas 📋
transaction cost	72139 gas 📋
input	0xa14...00000 📋

decoded input

```
{
    "address to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
    "uint256 tokenId": "0"
} 📋
```

decoded output   – 📋

logs

```
[
    {
        "from": "0xa373777C97B996A00E62497d85C781a2BEa38446",
        "topic": "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
        "event": "Transfer",
        "args": {
            "0": "0x0000000000000000000000000000000000000000",
            "1": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
            "2": "0",
            "from": "0x0000000000000000000000000000000000000000",
            "to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
            "tokenId": "0"
        }
    }
]
```

Transaction Details

Overview   Logs (2)

[This is a Polygon PoS **Testnet** transaction only]

⑦ Transaction Hash:	0xc540d4af547b6f15e0a3ff5fe4613d0149cf35a7b5c8c9b4620bca4a7668c0c7 ⧉
⑦ Status:	✓ Success
⑦ Block:	33218715 40 Block Confirmations
⑦ Timestamp:	🕐 1 min ago (Mar-17-2023 09:14:00 AM +UTC)
⑦ From:	0x3c4b0c4996968f8ab35d4e6790cc3b0dab59f272 ⧉
⑦ Interacted With (To):	Contract 0xa373777c97b99a00e62497d85c781a2bea38446 ✓ ⧉
⑦ Tokens Transferred:	▸ From 0x0000000000000… To 0x3c4b0c4996968… **For** ERC-721 TokenID [0] ⊙ StakeToken (STT)
⑦ Value:	0 MATIC ($0.00)
⑦ Transaction Fee:	0.000180347501154224 MATIC ($0.00)
⑦ Gas Price:	0.000000002500000016 MATIC (2.500000016 Gwei)

Click to see More ↓

発行したERC721をRaribleで確認

Rarible
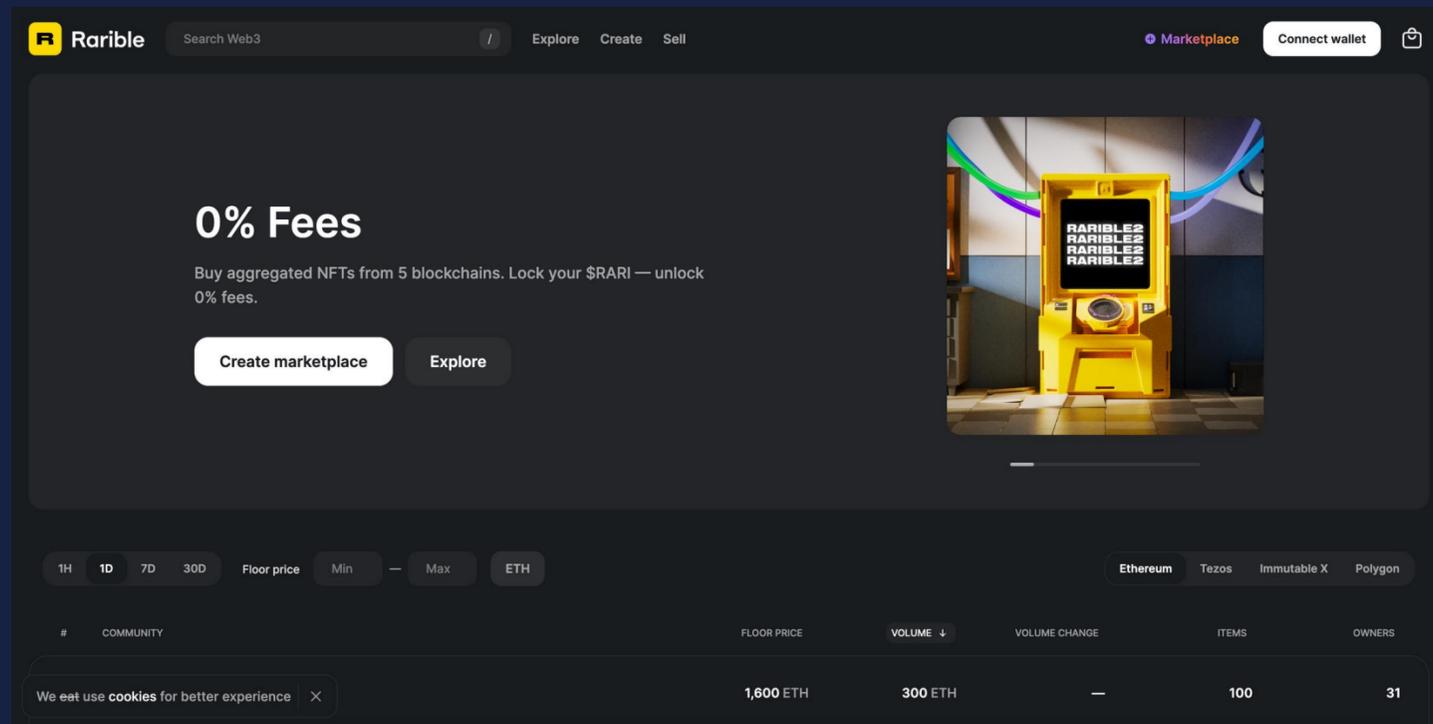
*Rarible*は世界最大の*NFT*マーケットプレイスの一つ

*NFT*マーケットプレイスはいわゆる
『NFTのECモール』であり、
誰もがコレクションを作成して販売可能。

*OpenSea*がメジャーではあるが、*Testnet*の不具合から
今回はRalibleを使用する。

↑ERC721のコントラクトアドレスを入れる

0% Fees

Buy aggregated NFTs from 5 blockchains. Lock your $RARI — unlock 0% fees.

Create marketplace · Explore

RARIBLE2
RARIBLE2
RARIBLE2
RARIBLE2

1H · **1D** · 7D · 30D · Floor price · Min — Max · ETH

Ethereum · Tezos · Immutable X · Polygon

#	COMMUNITY	FLOOR PRICE	VOLUME ↓	VOLUME CHANGE	ITEMS	OWNERS
		1,600 ETH	300 ETH	—	100	31

We ~~eat~~ use **cookies** for better experience ✕

< Filters   ⏸   **Live data active**
Last update: 20 minutes ago

🔍 Search by NFTs   Price: low to high ∨   ▦ ⦙⦙⦙

Status ∧

[All]   [Buy now]   [Not for sale]

Price ∧

Min   to   Max   MATIC ∨

Apply

Marketplace ∨

Properties ∨

We eat use **cookies** for better experience   ✕

Nothing found
We couldn't find anything with this
criteria

発行したERC721をRaribleで確認できない...?
発行されていることは分かるが、
画像データが表示されない...

Thinking Time

メタデータ（メタデータ自身もホスト先がHTTPかIPFS等かに分かれる）

```json
{
    "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
        }
    }
}
```

画像データ参照先

https://~

ipfs://
~

TokenID*を指定して
メタデータを参照

ブロックチェーン
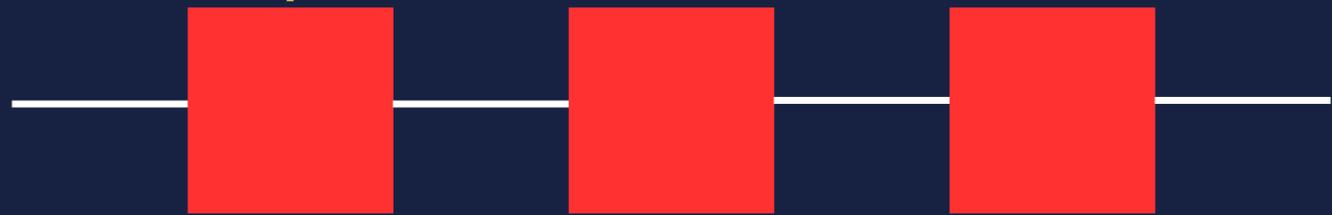
*TokenID：それぞれのトークンを指定する数字。

画像データ参照先ではなくメタデータを入れる必要がある

の設定を正しく行なってやり直してみよう。

ERC20 **ERC721** ERC1155   Governor   Custom   📋 Copy to Clipboard   ⊕ Open in Remix   ⬇ Download

SETTINGS

Name   Symbol

StakeToken   STT

Base URI   ❓

https://...

FEATURES

☑ Mintable   ❓
  └ ☐ Auto Increment Ids   ❓
☐ Burnable   ❓
☐ Pausable   ❓
☐ Votes   ❓
☐ Enumerable   ❓
☑ URI Storage   ❓

ACCESS CONTROL   ❓

◉ Ownable   ❓
○ Roles   ❓

UPGRADEABILITY ☐   ❓

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.9;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract StakeToken is ERC721, ERC721URIStorage, Ownable {
    constructor() ERC721("StakeToken", "STT") {}

    function safeMint(address to, uint256 tokenId, string memory uri)
        public
        onlyOwner
    {
        _safeMint(to, tokenId);
        _setTokenURI(tokenId, uri);
    }

    // The following functions are overrides required by Solidity.

    function _burn(uint256 tokenId) internal override(ERC721, ERC721URIStorage) {
        super._burn(tokenId);
    }

    function tokenURI(uint256 tokenId)
        public
        view
        override(ERC721, ERC721URIStorage)
        returns (string memory)
    {
        return super.tokenURI(tokenId);
    }
}
```

↑"image"にはPinataでIPFSにアップロードした画像のリンクを入れる

Pinata

- Files
- Gateways

DEVELOPERS

- API Keys
- Submarine Keys
- Access Controls
- Documentation

Upgrade plan

Files

Pin Status
Pinned

Filters

+ Add Files

Name	Content Identifier (CID)	Submarined		
test.json 👁 3/17/2023 189 B	QmX4PD9nk3BrWFNT3o53BPLL29Zi1q3M9j57sUg9zqLzXn 📋	False	Share	More
IMG_6928.png 👁 3/17/2023 17.97 MB	QmQcra56Qzg4BqoA3wJ2fTcHvDuzUR2FUEZcwnV4ADSi2K 📋	False	Share	More

‹ ›

[block:33221887 txIndex:4] from: 0x3C4...9f272 to: StakeToken.safeMint(address,uint256,string) 0x900...7b032 value: 0 wei data: 0xcd2...00000 logs: 1
hash: 0x12f...6ef53   **Debug** ∧

status	true Transaction mined and execution succeed
transaction hash	0xd6e1aabefa52e04fc6ea6de2384a43a0b2d776a8c7e2715f8d2fc83c0bb431a9
from	0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272
to	StakeToken.safeMint(address,uint256,string) 0x900E666246289aF5BC75C26A0Ba2BA0f4A07b032
gas	164206 gas
transaction cost	164206 gas
input	0xcd2...00000

decoded input

```
{
        "address to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
        "uint256 tokenId": "0",
        "string uri": "https://gateway.pinata.cloud/ipfs/QmX4PD9nk3BrWFNT3o53BPLL29Zi1q3M9j57sUg9zqLzXn"
}
```

decoded output   –

logs

```
[
        {
                "from": "0x900E666246289aF5BC75C26A0Ba2BA0f4A07b032",
                "topic": "0xddf252ad1be2c89b69c2b068fc378daa952ba7f163c4a11628f55a4df523b3ef",
                "event": "Transfer",
                "args": {
                        "0": "0x0000000000000000000000000000000000000000",
                        "1": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
                        "2": "0",
                        "from": "0x0000000000000000000000000000000000000000",
                        "to": "0x3C4b0C4996968f8ab35D4E6790CC3B0DAb59f272",
                        "tokenId": "0"
                }
        }
]
```

Search Web3 /

Explore   Create   Sell

Marketplace   Connect wallet

StakeToken

Created by **0×3c4b0...f272**   Address **0×900...b032**

Create marketplace   Place a bid for any NFT from this collection   Place a bid

Floor —

Volume   **0 MATIC**

Items   **1**

Owners   **1**

Blockchain   **Polygon**

Items   Activity

Live data active

We eat use **cookies** for better experience ✕

Search by NFTs

Price: low to high ⌄

*ERC721*発行 終