



Blockchain #16

NFT and DeFi

Prof. Byung Il Kwak



- ❑ Basic token
- ❑ Ethereum Improvement Proposals
- ❑ ERC 20
- ❑ ERC 721

- NFT

- DeFi

- Oracle

CONTENTS

- ❑ NFT (Non-Fungible Token)

Non-Fungible Token (NFT)

- 스마트 계약내에서 NFT를 위한 표준 API 구현을 수행 (NFT \approx Assets)
- ERC-721 표준은 NFT를 추적하고 전송하는 기본 기능을 제공함
 - ▣ 물리적 자산 — 예) 주택, 독특한 예술품
 - ▣ 가상 수집품 — 예) 고양이 사진, 수집 가능한 카드
 - ▣ “음수 값” 자산 — 예) 대출

Non-Fungible Token (NFT)

□ NFT

- 한 개의 토큰을 다른 토큰으로 대체하는 것이 불가능한 암호화폐
 - 조작이 불가능하도록 디지털 자산의 소유권을 증명하고 보호하는 기술
 - 즉, 디지털파일(그림, 음악 등)을 블록체인 네트워크에 NFT로 기록하면, 디지털파일의 원본에 대한 소유권을 증명할 수 있음
- 메인넷을 이더리움으로 할 경우, ERC721을 기반으로 작성
- 메인넷을 클레이튼으로 할 경우, K~ 기반으로 작성

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721

- [openzeppelin-contracts/contracts/token/ERC721 at master · OpenZeppelin/openzeppelin-contracts · GitHub](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/ERC721.sol)

```
447 lines (391 sloc) | 13.9 KB
1 // SPDX-License-Identifier: MIT
2 // OpenZeppelin Contracts v4.4.0 (token/ERC721/ERC721.sol)
3
4 pragma solidity ^0.8.0;
5
6 import "./IERC721.sol";
7 import "./IERC721Receiver.sol";
8 import "./extensions/IERC721Metadata.sol";
9 import "./utils/Address.sol";
10 import "./utils/Context.sol";
11 import "./utils/Strings.sol";
12 import "./utils/introspection/ERC165.sol";
13
14 /**
15  * @dev Implementation of https://eips.ethereum.org/EIPS/eip-721[ERC721] Non-Fungible Token Standard, including
16  * the metadata extension, but not including the Enumerable extension, which is available separately as
17  * (ERC721Enumerable).
18  */
19 contract ERC721 is Context, ERC165, IERC721, IERC721Metadata {
20     using Address for address;
21     using Strings for uint256;
22
23     // Token name
24     string private _name;
25
26     // Token symbol
27     string private _symbol;
28
29     // Mapping from token ID to owner address
30     mapping(uint256 => address) private _owners;
31
32     // Mapping owner address to token count
33     mapping(address => uint256) private _balances;
34
35     // Mapping from token ID to approved address
36     mapping(uint256 => address) private _tokenApprovals;
37
38     // Mapping from owner to operator approvals
39     mapping(address => bool) private _operatorApprovals;
40
41     /**
42     * @dev Initializes the contract by setting a 'name' and a 'symbol' to the token collection.
43     */
44     constructor(string memory name_, string memory symbol_) {
45         _name = name_;
46         _symbol = symbol_;
47     }
48
49     /**
50     * @dev See (IERC165-supportsInterface).
51     */
52     function supportsInterface(bytes4 interfaceId) public view virtual override(ERC165, IERC165) returns (bool) {
53         return
54             interfaceId == type(IERC721).interfaceId ||
55             interfaceId == type(IERC721Metadata).interfaceId ||
56             super.supportsInterface(interfaceId);
57     }
58 }
```

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721

- Openzeppelin에서 ERC 721에 구현해야 할 인터페이스들을 소스코드로 제공함
- 공식 EIP 문서에는 주석으로 각 함수가 수행해야 하는 기능들에 대해 명시가 되어 있음

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 1

ERC 721
Interface

```
/// @notice Count all NFTs assigned to an owner
/// @dev NFTs assigned to the zero address are considered invalid, and this
/// function throws for queries about the zero address.
/// @param _owner An address for whom to query the balance
/// @return The number of NFTs owned by `_owner`, possibly zero
function balanceOf(address _owner) external view returns (uint256);
```

ERC 721
Code

```
/**
 * @dev See {IERC721-balanceOf}.
 */
function balanceOf(address owner) public view virtual override returns (uint256) {
    require(owner != address(0), "ERC721: balance query for the zero address");
    return _balances[owner];
}
```

function balanceOf(address _owner)는 변수로 받는 '_owner' 주소가
보유하고 있는 NFT 토큰들 개수를 나타냄

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 2

ERC 721
Interface

```
/// @notice Find the owner of an NFT
/// @dev NFTs assigned to zero address are considered invalid, and queries
/// about them do throw.
/// @param _tokenId The identifier for an NFT
/// @return The address of the owner of the NFT
function ownerOf(uint256 _tokenId) external view returns (address);
```

ERC 721
Code

```
/**
 * @dev See {IERC721-ownerOf}.
 */
function ownerOf(uint256 tokenId) public view virtual override returns (address) {
    address owner = _owners[tokenId];
    require(owner != address(0), "ERC721: owner query for nonexistent token");
    return owner;
}
```

`function ownerOf(uint256 _tokenId)`는 해당 NFT 토큰의 ID를 변수로 받아 NFT 토큰을 소유하고 있는 주소를 반환함

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 3

ERC 721
Interface

```
/// @notice Change or reaffirm the approved address for an NFT
/// @dev The zero address indicates there is no approved address.
/// Throws unless `msg.sender` is the current NFT owner, or an authorized
/// operator of the current owner.
/// @param _approved The new approved NFT controller
/// @param _tokenId The NFT to approve
function approve(address _approved, uint256 _tokenId) external payable;
```

ERC 721
Code

```
function approve(address to, uint256 tokenId) public virtual override {
    address owner = ERC721.ownerOf(tokenId);
    require(to != owner, "ERC721: approval to current owner");

    require(
        _msgSender() == owner || isApprovedForAll(owner, _msgSender()),
        "ERC721: approve caller is not owner nor approved for all"
    );

    _approve(to, tokenId);
}
```

`function approve(address _approved, uint256 _tokenId)`는 해당 주소에 NFT 토큰 전송 권한을 부여하는 기능 (토큰을 보유하고 있는 사람이 `_tokenId`와 Operator의 address를 입력하면 Operator에게 해당 토큰 거래를 허용하는 기능을 수행)

* Operator는 토큰을 대신 전송하는 사람을 의미함.

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 4

ERC 721
Interface

```
/// @notice Get the approved address for a single NFT
/// @dev Throws if `_tokenId` is not a valid NFT.
/// @param _tokenId The NFT to find the approved address for
/// @return The approved address for this NFT, or the zero address if there is none
function getApproved(uint256 _tokenId) external view returns (address);
```

ERC 721
Code

```
/**
 * @dev See {IERC721-getApproved}.
 */
function getApproved(uint256 tokenId) public view virtual override returns (address) {
    require(_exists(tokenId), "ERC721: approved query for nonexistent token");

    return _tokenApprovals[tokenId];
}
```

`function getApproved(uint256 _tokenId)`는 해당 NFT 토큰의 ID를 입력 변수로 받아, 그 토큰에 해당하는 Operator를 반환함.

* Operator는 토큰을 대신 전송하는 사람을 의미함.

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 5

ERC 721 Interface

```
/// @notice Enable or disable approval for a third party ("operator") to manage
/// all of `msg.sender`'s assets
/// @dev Emits the ApprovalForAll event. The contract MUST allow
/// multiple operators per owner.
/// @param _operator Address to add to the set of authorized operators
/// @param _approved True if the operator is approved, false to revoke approval
function setApprovalForAll(address _operator, bool _approved) external;
```

ERC 721 Code

```
/**
 * @dev See {IERC721-setApprovalForAll}.
 */
function setApprovalForAll(address operator, bool approved) public virtual override {
    _setApprovalForAll(_msgSender(), operator, approved);
}
```

`function setApprovalForAll(address _operator, bool _approved)`는 NFT 토큰 소유자가 해당 주소에게 모든 NFT 토큰에 대한 전송 권한을 부여 또는 해제하는 기능을 수행 ('_approved'가 True일 경우 모든 토큰에 대한 전송 권한을 가지며, False일 경우 모든 토큰에 대한 전송 권한을 취소하게 됨)

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 6

ERC 721
Interface

```
/// @notice Query if an address is an authorized operator for another address
/// @param _owner The address that owns the NFTs
/// @param _operator The address that acts on behalf of the owner
/// @return True if `_operator` is an approved operator for `_owner`, false otherwise
function isApprovedForAll(address _owner, address _operator) external view returns (bool);
```

ERC 721
Code

```
/**
 * @dev See {IERC721-isApprovedForAll}.
 */
function isApprovedForAll(address owner, address operator) public view virtual override returns (bool) {
    return _operatorApprovals[owner][operator];
}
```

function `isApprovedForAll(address _owner, address _operator)`는 '`_owner`' 주소가 `function setApprovalForAll()` 의 권한이 있는지를 'True/False'로 보여줌

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 7

ERC 721
Interface

```
/// @notice Transfer ownership of an NFT -- THE CALLER IS RESPONSIBLE
/// TO CONFIRM THAT `_to` IS CAPABLE OF RECEIVING NFTS OR ELSE
/// THEY MAY BE PERMANENTLY LOST
/// @dev Throws unless `msg.sender` is the current owner, an authorized
/// operator, or the approved address for this NFT. Throws if `_from` is
/// not the current owner. Throws if `_to` is the zero address. Throws if
/// `_tokenId` is not a valid NFT.
/// @param _from The current owner of the NFT
/// @param _to The new owner
/// @param _tokenId The NFT to transfer
function transferFrom(address _from, address _to, uint256 _tokenId) external payable;
```

ERC 721
Code

```
/**
 * @dev See {IERC721-transferFrom}.
 */
function transferFrom(
    address from,
    address to,
    uint256 tokenId
) public virtual override {
    //solhint-disable-next-line max-line-length
    require(!_isApprovedOrOwner(_msgSender(), tokenId), "ERC721: transfer caller is not owner nor approved");

    _transfer(from, to, tokenId);
}
```

function transferFrom(address _from, address _to, uint256 _tokenId)는 NFT
토큰 소유자로부터('from') 해당 NFT 토큰을 다른 주소로('_to') 전송함

Non-Fungible Token (NFT)

□ NFT 설계

▣ ERC 721 코드 리뷰 - 8

ERC 721
Interface

```
/// @notice Transfers the ownership of an NFT from one address to another address
/// @dev This works identically to the other function with an extra data parameter,
/// except this function just sets data to "".
/// @param _from The current owner of the NFT
/// @param _to The new owner
/// @param _tokenId The NFT to transfer
function safeTransferFrom(address _from, address _to, uint256 _tokenId) external payable;
```

ERC 721
Code

```
/**
 * @dev See {IERC721-safeTransferFrom}.
 */
function safeTransferFrom(
    address from,
    address to,
    uint256 tokenId
) public virtual override {
    safeTransferFrom(from, to, tokenId, "");
}

/**
 * @dev See {IERC721-safeTransferFrom}.
 */
function safeTransferFrom(
    address from,
    address to,
    uint256 tokenId,
    bytes memory _data
) public virtual override {
    require(_isApprovedOrOwner(_msgSender(), tokenId), "ERC721: transfer caller is not owner nor approved");
    _safeTransfer(from, to, tokenId, _data);
}
```

function safeTransferFrom(address _from, address _to, uint256 _tokenId)는
전송받은 ('_to') 주소가 ERC 721 토큰을 받을 수 있는지 체크하고 전송하는 함수

Non-Fungible Token (NFT)

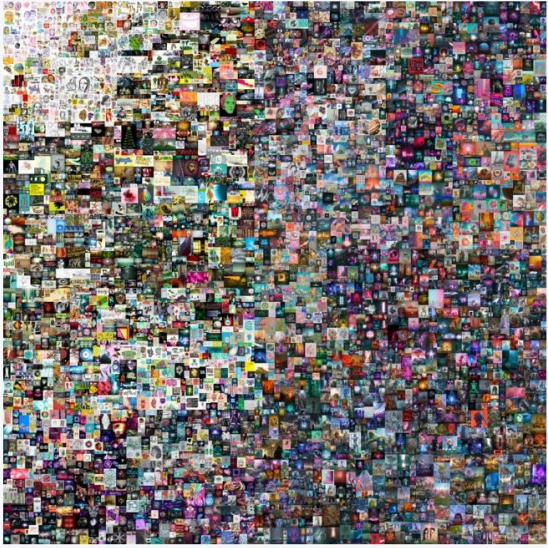
❑ Everyday: The First 5000 Day

CHRISTIE'S Auctions Private Sales Locations Departments Stories Services

Search by lot or keyword

COVID-19 Important notice

< 25 Feb - 11 Mar 2021 | Online Auction 20447 Beeple | The First 5000 Days > Lot 1



* Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS

Price Realised
USD 69,346,250

Estimate unknown

Closed: 12 Mar 2021

Save Share

Details

Lot Essay

Related Articles

More from

Details

Beeple (b. 1981)

EVERYDAYS: THE FIRST 5000 DAYS

token ID: 40913

wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807

smart contract address: 0x2a46f2fd99e19a89476e2f62270e0a35bbf075c

non-fungible token (jpg)

21,069 x 21,069 pixels (319,168,313 bytes)

Minted on 16 February 2021. This work is unique.

Brought to you by



Noah Davis
Associate Vice President, Specialist

A Christie's specialist may contact you to discuss this lot or to notify you if the condition changes prior to the sale.

NDavis@christies.com
[+1 212 468 7173](tel:+12124687173)

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

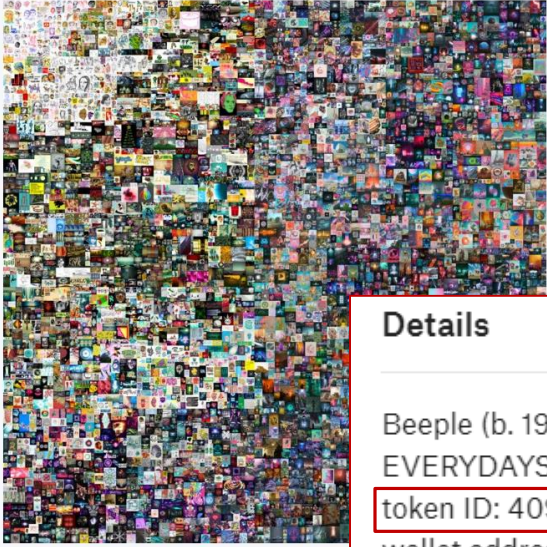
CHRISTIE'S Auctions Private Sales Locations Departments Stories Services

Search by lot or keyword

COVID-19 Important notice

25 Feb - 11 Mar 2021 | Online Auction 20447 Beeple | The First 5000 Days

Lot 1



Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS

Price Realised
USD 69,346,250

Estimate unknown

Closed: 12 Mar 2021

Save Share

Details

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)
21,069 x 21,069 pixels (319,168,313 bytes)
Minted on 16 February 2021. This work is unique.

Details

Lot Essay

Related Articles

More from

Beeple (b. 1981)
EVERYDAYS: THE FIRST 5000 DAYS
token ID: 40913
wallet address: 0xc6b0562605D35eE710138402B878ffe6F2E23807
smart contract address: 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756
non-fungible token (jpg)
21,069 x 21,069 pixels (319,168,313 bytes)
Minted on 16 February 2021. This work is unique.

A Christie's specialist may contact you to discuss this lot or to notify you if the condition changes prior to the sale.
NDavis@christies.com
+1 212 468 7173

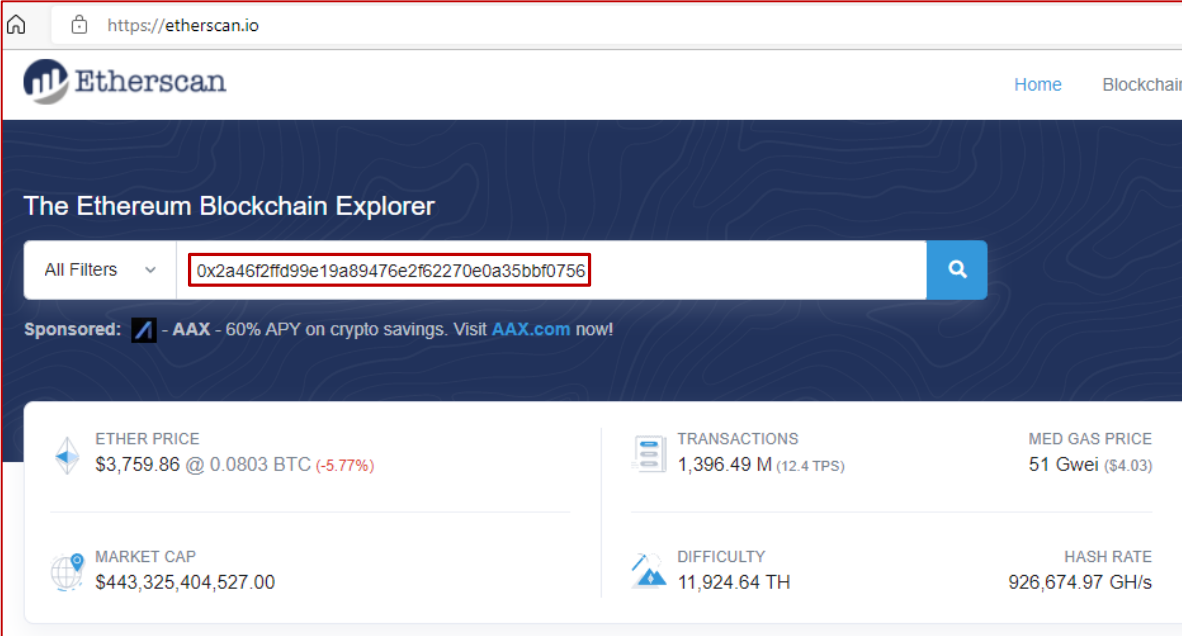
Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day







❑ Token ID: 40913

❑ Smart Contract Address:

– 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756



The screenshot shows the Etherscan website, "The Ethereum Blockchain Explorer". The search bar contains the address `0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756`, which is highlighted with a red box. Below the search bar, there is a sponsored banner for AAX. The main content area displays various Ethereum statistics:

| ETHER PRICE | | TRANSACTIONS | | MED GAS PRICE | |
|---|----------------------------------|---|-----------------------|---|------------------|
|  | \$3,759.86 @ 0.0803 BTC (-5.77%) |  | 1,396.49 M (12.4 TPS) |  | 51 Gwei (\$4.03) |
| MARKET CAP | | DIFFICULTY | | HASH RATE | |
|  | \$443,325,404,527.00 |  | 11,924.64 TH |  | 926,674.97 GH/s |

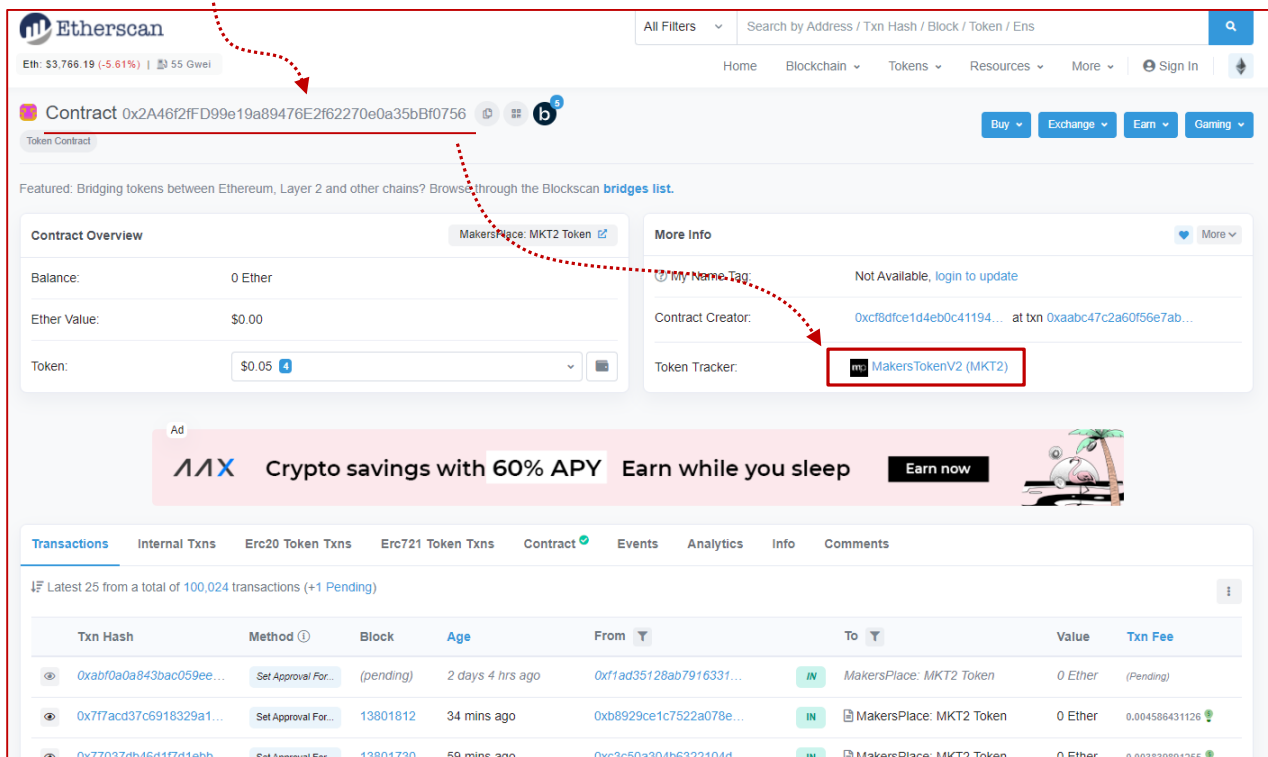
Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

❑ Token ID: 40913

❑ Smart Contract Address:

– 0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756



Etherscan
Eth: \$3,766.19 (-5.61%) | 55 Gwei

Contract: 0x2A46f2fD99e19a89476E2f62270e0a35bBf0756

Token Contract

Featured: Bridging tokens between Ethereum, Layer 2 and other chains? Browse through the Blockscan [bridges list](#).

Contract Overview

Balance: 0 Ether

Ether Value: \$0.00

Token: \$0.05

More Info

My Name Tag: Not Available, [login to update](#)

Contract Creator: 0xcf8dfce1d4eb0c41194... at txn 0xaabc47c2a60f56e7ab...

Token Tracker: **MakersTokenV2 (MKT2)**

Ad
MAX Crypto savings with 60% APY Earn while you sleep [Earn now](#)

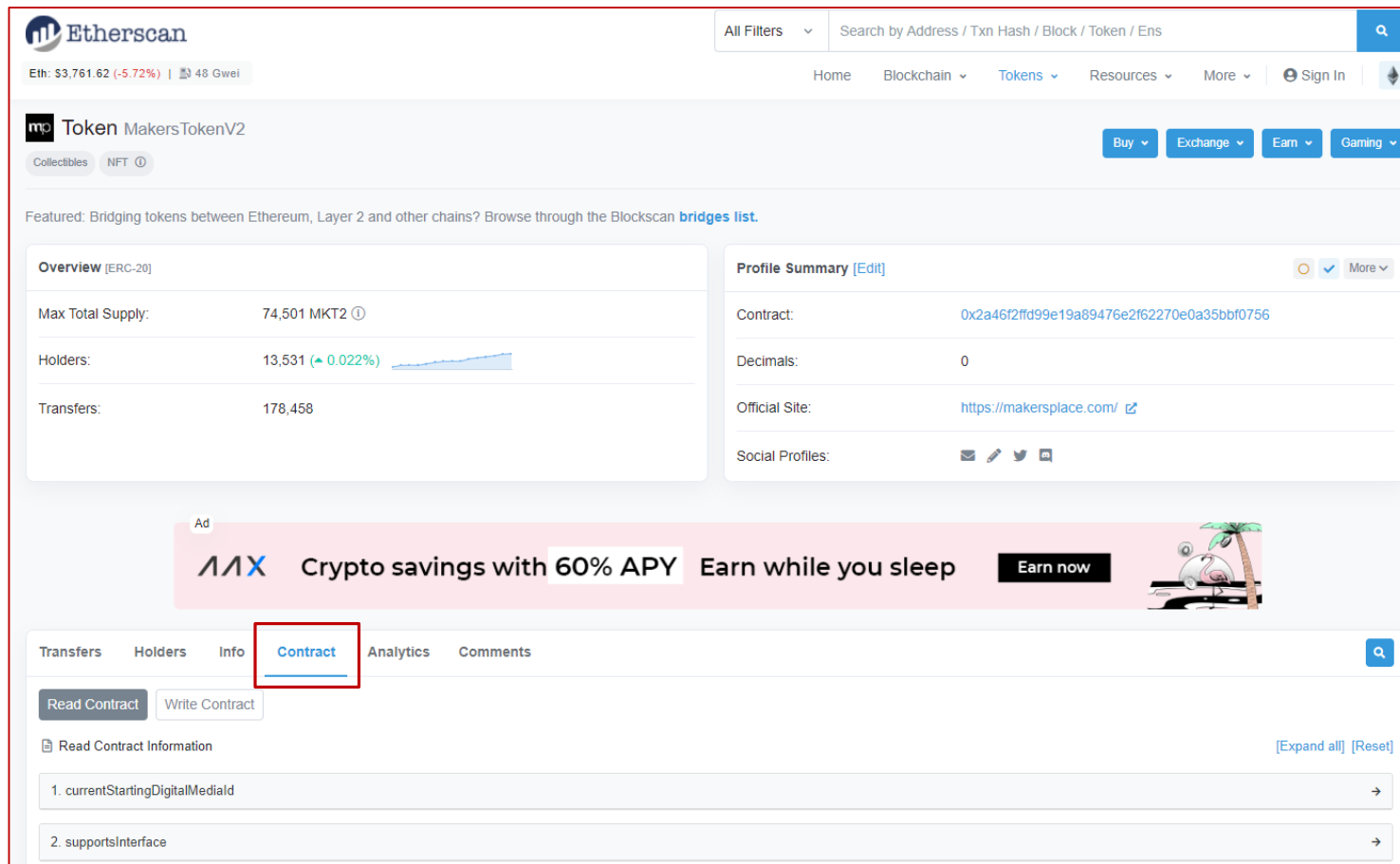
Transactions Internal Txns Erc20 Token Txns Erc721 Token Txns Contract Events Analytics Info Comments

Latest 25 from a total of 100,024 transactions (+1 Pending)

| Txn Hash | Method | Block | Age | From | To | Value | Txn Fee |
|-------------------------|---------------------|-----------|------------------|--------------------------|-------------------------|---------|----------------|
| 0xabf0a0a843bac059ee... | Set Approval For... | (pending) | 2 days 4 hrs ago | 0xf1ad35f128ab791633f... | MakersPlace: MKT2 Token | 0 Ether | (Pending) |
| 0x7f7acd37c6918329a1... | Set Approval For... | 13801812 | 34 mins ago | 0xb8929ce1c7522a078e... | MakersPlace: MKT2 Token | 0 Ether | 0.004586431126 |
| 0x77037db46d1f741ebh | Set Approval For... | 13801730 | 59 mins ago | 0xc3c50a304b6322104d | MakersPlace: MKT2 Token | 0 Ether | 0.00383881255 |

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day



The screenshot shows the Etherscan interface for the MakersTokenV2 token. The top navigation bar includes the Etherscan logo, a search bar, and links for Home, Blockchain, Tokens, Resources, and More. The token page header shows the token name, a 'Buy' button, and an 'Exchange' button. The main content area is divided into two columns. The left column, titled 'Overview [ERC-20]', displays the Max Total Supply (74,501 MKT2), Holders (13,531, up 0.022%), and Transfers (178,458). The right column, titled 'Profile Summary [Edit]', shows the Contract address (0x2a46f2ffd99e19a89476e2f62270e0a35bbf0756), Decimals (0), Official Site (https://makersplace.com/), and Social Profiles. Below these columns is an advertisement for AAX Crypto savings with 60% APY. At the bottom, the 'Contract' tab is selected, showing a list of contract functions: 1. currentStartingDigitalMediaId and 2. supportsInterface. A red box highlights the 'Contract' tab and the function list.

| Function | Value |
|-------------------------------|-------|
| currentStartingDigitalMediaId | |
| supportsInterface | |



23. tokenURI →

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

23. tokenURI

_tokenId (uint256)

40913

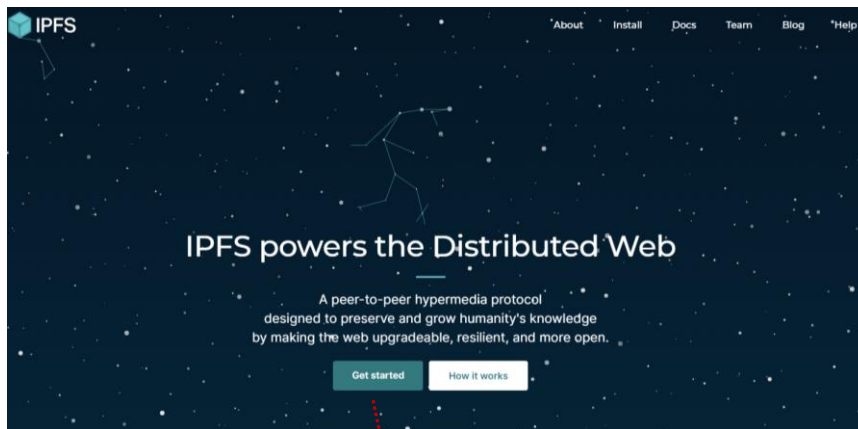
Query

↓

[tokenURI(uint256) method Response]

>> string : ipfs://ipfs/QmPAg1mjxcEQPPtqsLoEcauVedaeMH81WXPpPx3VC5zUz


❑ IPFS



Install IPFS

future of the web right now — just choose the option that's right for you.

Store and provide files



IPFS Desktop

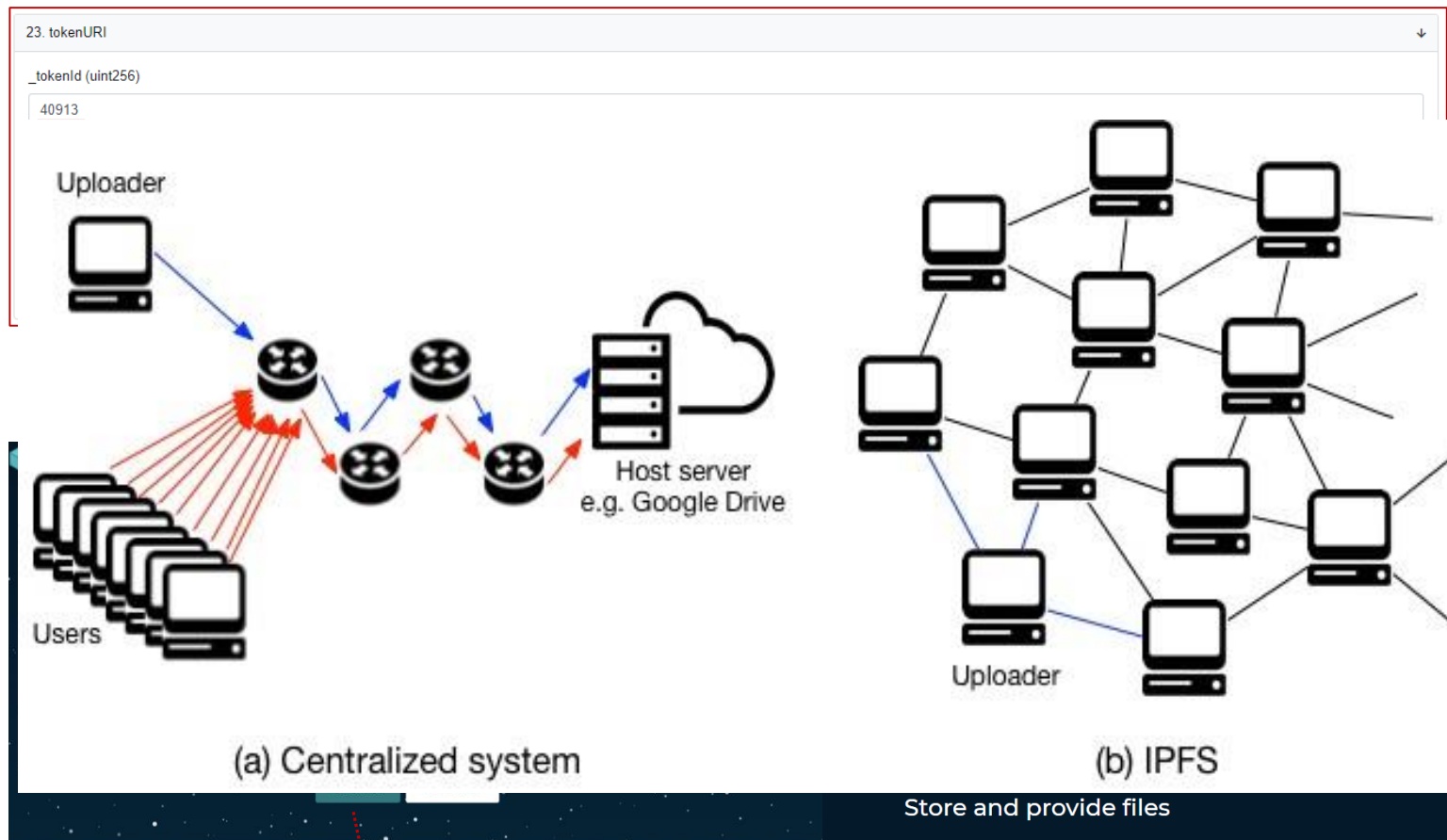
IPFS for everyone

The IPFS Desktop app offers menubar/tray shortcuts and an easy interface for adding, pinning, and sharing files — plus a full IPFS node ready for heavy-duty hosting and development. Great for developers and less experienced users alike.

Install IPFS Desktop

➔ Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day



IPFS Desktop
IPFS for everyone

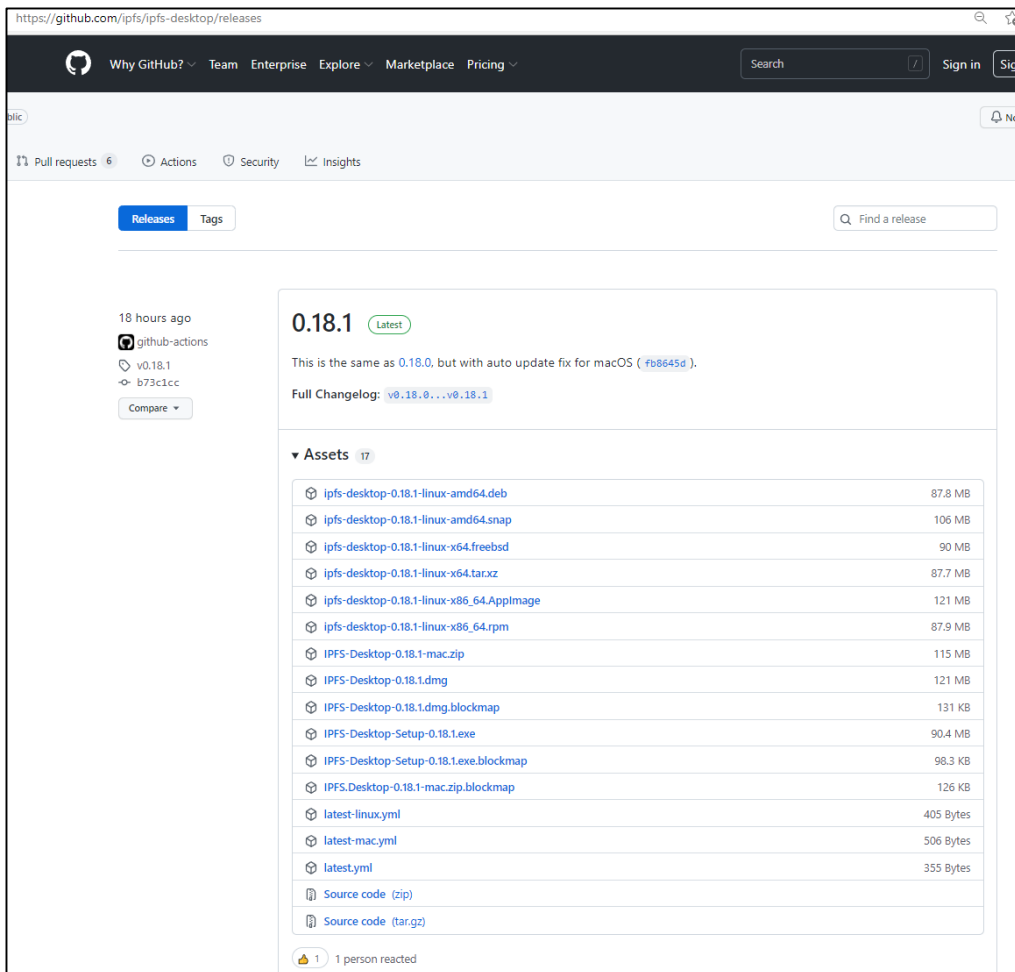
The IPFS Desktop app offers menubar/tray shortcuts and an easy interface for adding, pinning, and sharing files — plus a full IPFS node ready for heavy-duty hosting and development. Great for developers and less experienced users alike.

Install IPFS Desktop

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

❑ IPFS



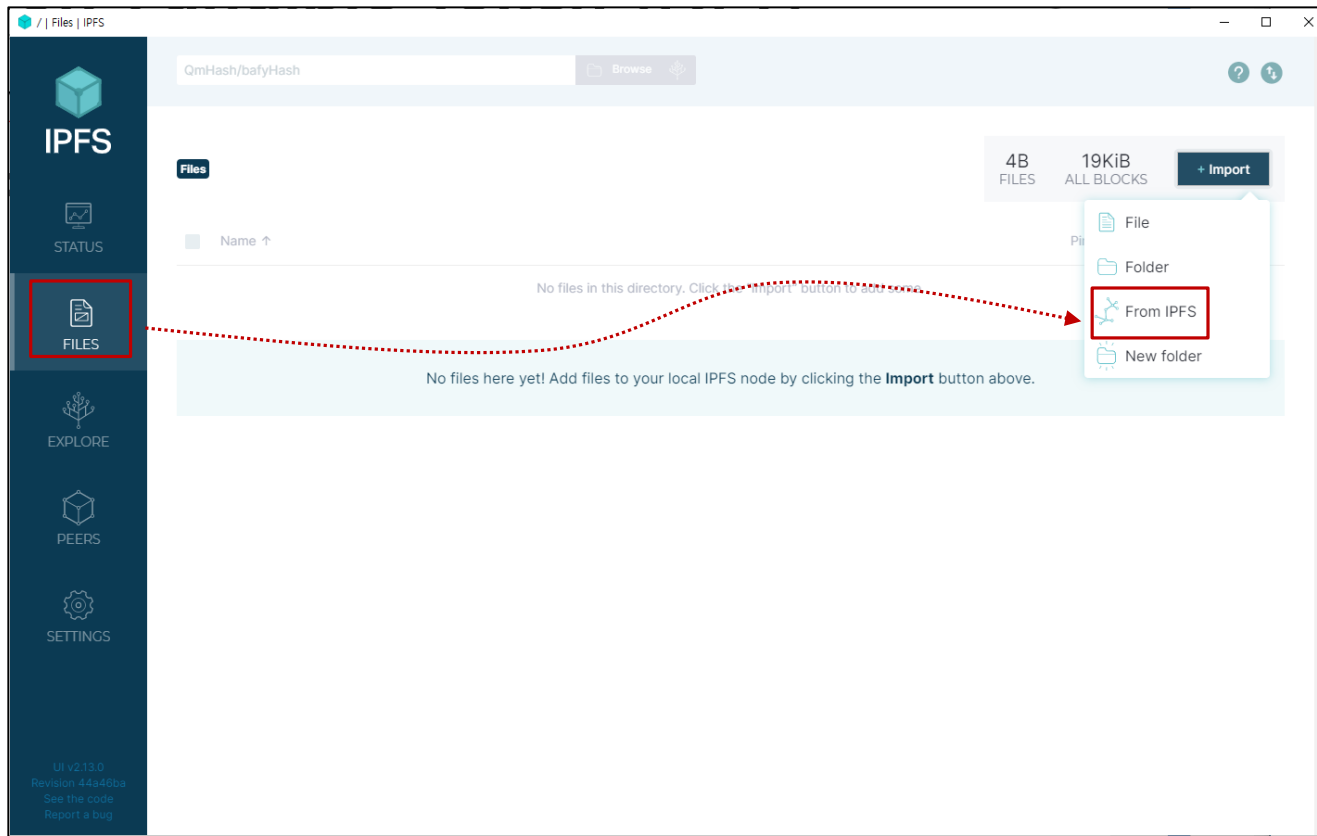
The screenshot shows the GitHub release page for the repository `ipfs/ipfs-desktop`. The page displays the latest release, **0.18.1**, which was published 18 hours ago. The release notes indicate that this version is the same as 0.18.0 but includes an auto-update fix for macOS. A full changelog is provided, showing updates from `v0.18.0...v0.18.1`. The assets section lists 17 downloadable files, including desktop binaries for Linux (deb, snap, tar.xz), macOS (zip, dmg), and Windows (exe, blockmap), as well as source code (zip, tar.gz) and configuration files (yaml).

| Asset | Size |
|---|-----------|
| ipfs-desktop-0.18.1-linux-amd64.deb | 87.8 MB |
| ipfs-desktop-0.18.1-linux-amd64.snap | 106 MB |
| ipfs-desktop-0.18.1-linux-x64.freebsd | 90 MB |
| ipfs-desktop-0.18.1-linux-x64.tar.xz | 87.7 MB |
| ipfs-desktop-0.18.1-linux-x86_64.AppImage | 121 MB |
| ipfs-desktop-0.18.1-linux-x86_64.rpm | 87.9 MB |
| IPFS-Desktop-0.18.1-mac.zip | 115 MB |
| IPFS-Desktop-0.18.1.dmg | 121 MB |
| IPFS-Desktop-0.18.1.dmg.blockmap | 131 KB |
| IPFS-Desktop-Setup-0.18.1.exe | 90.4 MB |
| IPFS-Desktop-Setup-0.18.1.exe.blockmap | 98.3 KB |
| IPFS.Desktop-0.18.1-mac.zip.blockmap | 126 KB |
| latest-linux.yml | 405 Bytes |
| latest-mac.yml | 506 Bytes |
| latest.yml | 355 Bytes |
| Source code (zip) | |
| Source code (tar.gz) | |

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

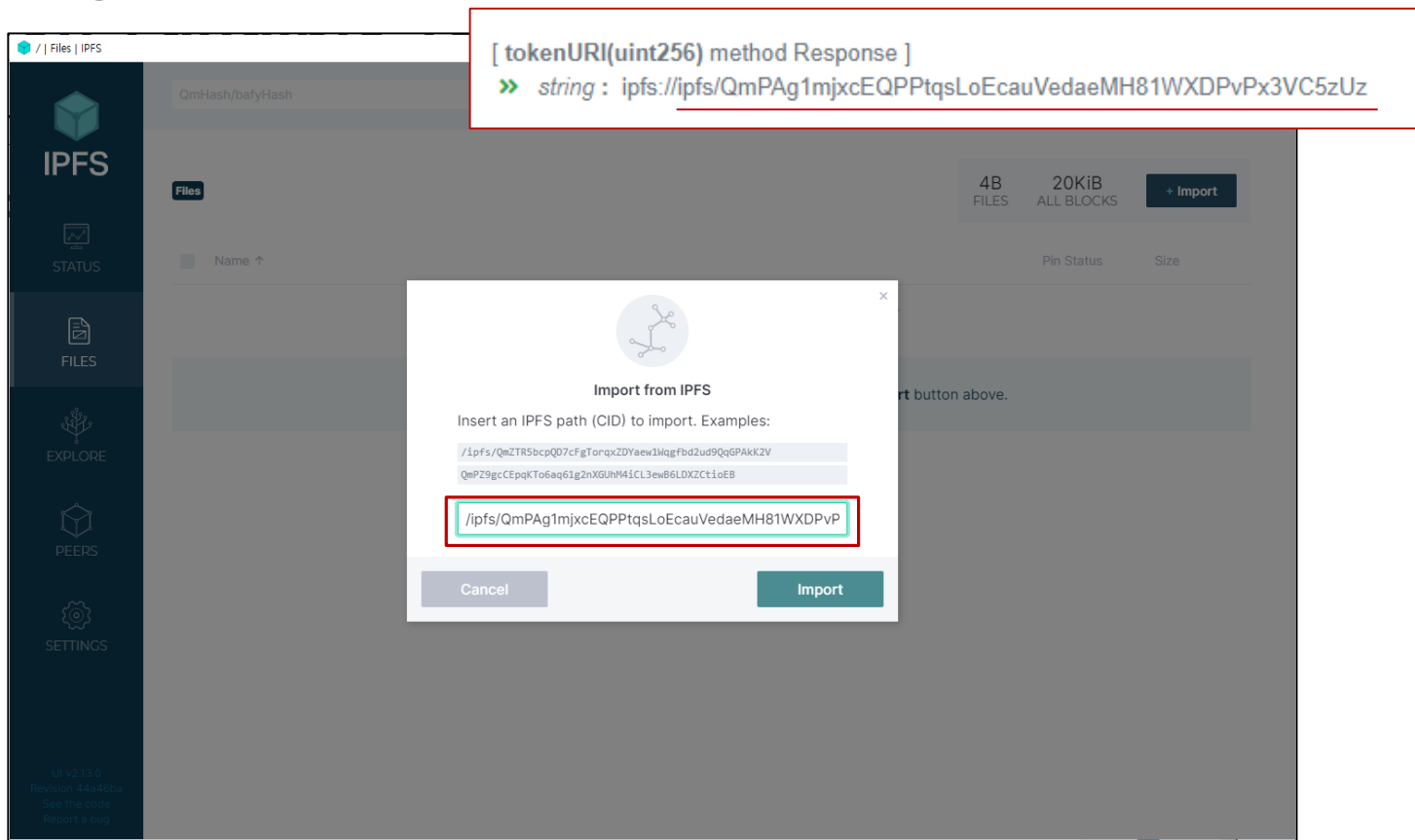
❑ IPFS



Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

❑ IPFS



[tokenURI(uint256) method Response]
>> string : ipfs://ipfs/QmPag1mjxcEQPPtqsLoEcauVedaeMH81WXPvPx3VC5zUz

IPFS

Files

4B FILES 20KiB ALL BLOCKS + Import

Import from IPFS

Insert an IPFS path (CID) to import. Examples:

/ipfs/QmZTR5bcpQD7cFgTorqxZDYaew1MqgFbd2ud9QgPakk2V
QmPZ9gcCEpqKTo6aq61g2nXGJH41CL3ewB6LDXZCtIoEB

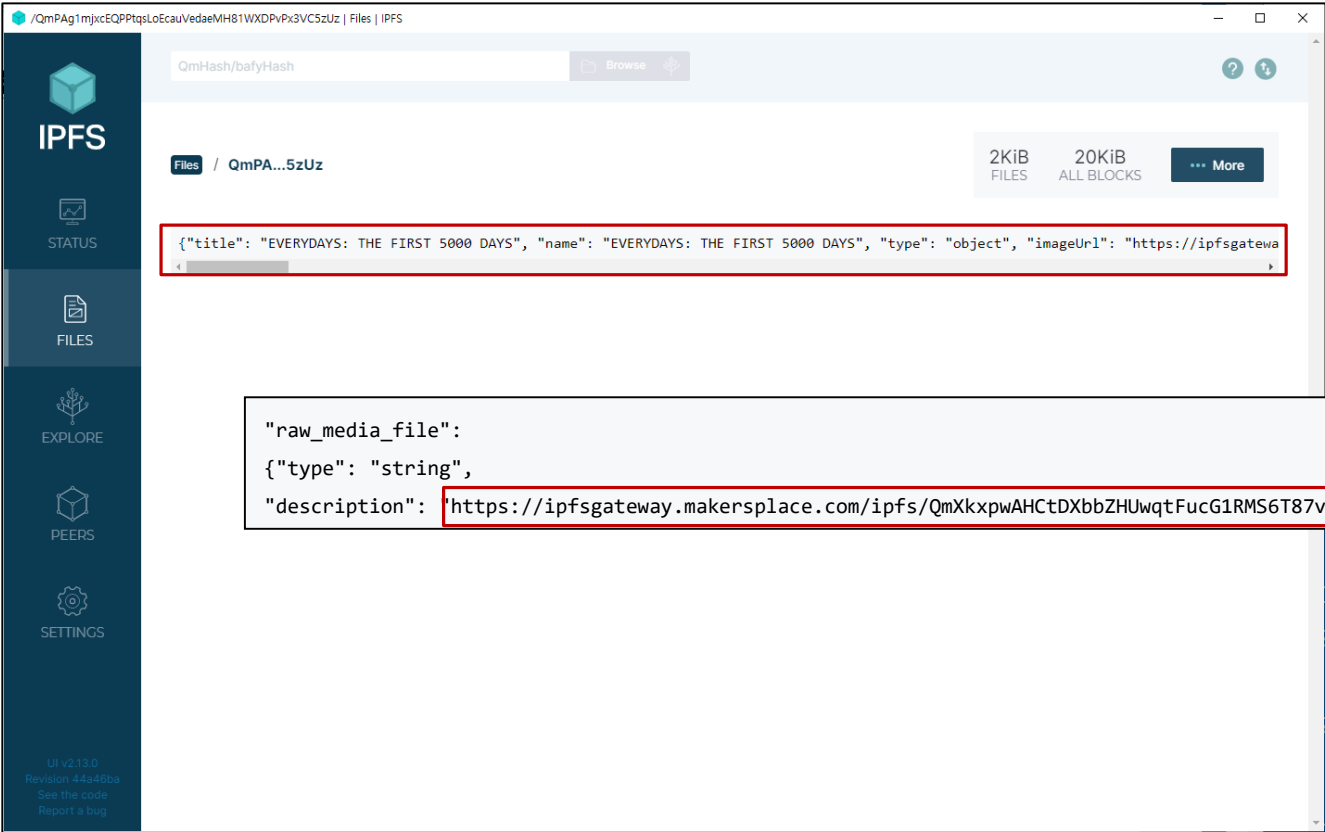
/ipfs/QmPag1mjxcEQPPtqsLoEcauVedaeMH81WXPvP

Cancel Import

Non-Fungible Token (NFT)

❑ Everyday: The First 5000 Day

❑ IPFS



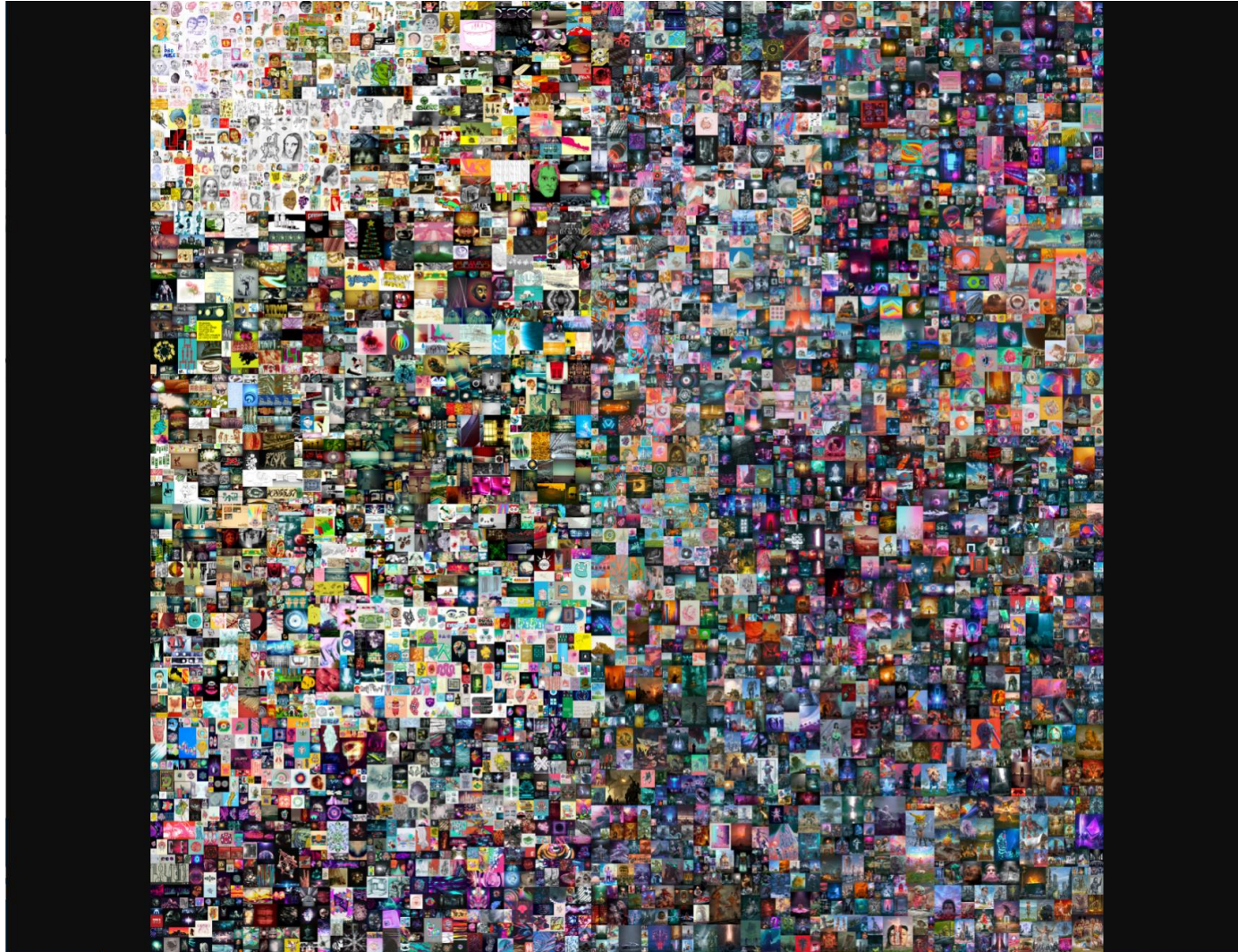
The screenshot shows the IPFS web interface. The left sidebar contains navigation links: IPFS, STATUS, FILES, EXPLORE, PEERS, and SETTINGS. The main content area displays the file details for 'QmPA...5zUz'. The file is 2KiB in size and is an object type. The metadata is shown in a JSON format, with the 'imageUri' field highlighted in red. The description field is also highlighted in red, showing the URL 'https://ipfsgateway.makersplace.com/ipfs/QmXkxpWAHctDXbbZHUwqtFucG1RMS6T87vi1CdvdL7qA'.

```
{
  "title": "EVERYDAYS: THE FIRST 5000 DAYS",
  "name": "EVERYDAYS: THE FIRST 5000 DAYS",
  "type": "object",
  "imageUri": "https://ipfsgatewa"
}
```

```
{
  "raw_media_file": {
    "type": "string",
    "description": "https://ipfsgateway.makersplace.com/ipfs/QmXkxpWAHctDXbbZHUwqtFucG1RMS6T87vi1CdvdL7qA"
  }
}
```

Non-Fungible Token (NFT)

□ Everyday: The First 5000 Day



Non-Fungible Token (NFT)

□ NFT

- ▣ 결국 원본이 저장된 곳의 인터넷 주소에 대해서만 가지고 있음
- ▣ 실제 파일은 블록체인 외부의 별도 저장매체에 보관되어 있음 (IPFS)
- ▣ 즉, NFT 자체는 블록체인에 증서만 보관될 뿐 파일 자체는 보관하지 않음

□ NFT 관련 중요점

- ▣ NFT 메타 데이터에 표시된 디지털 콘텐츠 원본 확인
- ▣ NFT 거래 시, 거래 당사자가 디지털 콘텐츠 원본의 소유주인지를 확인
- ▣ NFT 생성 및 이를 블록체인에 등록하는 과정에서 저작권 침해가 발생할 수 있음
- ▣ NFT가 원본과 보복사본을 구별 가능하게는 해주지만, 원본에 대한 무단 복제 자체를 막지 못함

Non-Fungible Token (NFT)

□ NFT 특징

- ▣ 스마트 컨트랙트와 연동하여 개인간 거래(P2P)를 가능하게 함
- ▣ NFT는 탈중앙화된 블록체인상에 저장되므로, 위조가 어렵고 추적하기 쉬움. 또한, 소유권 분실에 대한 우려가 적음
- ▣ 토큰을 분할하여 소유권을 부분적으로 유통 가능하도록 함
- ▣ NFT는 매체에 대한 소유권을 의미함.(저작권을 의미하지 않음)
 - 타인의 저작물에 대한 NFT 생성시 문제가 될 수 있음

Non-Fungible Token (NFT)

□ NFT 현황 및 활용 사례

▣ 실제 비즈니스에 이용하는 NFT 사례

〈 NFT 도입 연구 기업 및 관련 비즈니스 사례 〉

| 분야 | 기업명 | NFT 관련 비즈니스 |
|-------------|--------------------|--------------------------------|
| 스포츠 | NBA | NBA Top Shot |
| | MLB | MLB Champions |
| | Formula 1 | F1 Delta Time |
| 패션 | NIKE | CryptoKicks |
| | LVMH | 명품의 진위를 증명하기 위한 블록체인 'AURA' 출시 |
| | BREITLING | NFT를 포함하는 이더리움 시스템으로 정품 인증 |
| 엔터테인먼트 & 영화 | Turner Sports | Blocklete Games |
| | Warner Music Group | 블록체인 기반 게임업체 Dapper Labs에 투자 |
| 테크 & 인프라 | AMD | Robotcache BGA와 파트너십 |
| | Microsoft | Azure Heroes |
| | IBM | NFT 지원 커스텀 블록체인 |
| | HTC | Exodus 1 |
| | 삼성 | NFT 지원 전자지갑 |
| 비디오 게임 | Ubisoft | Rabbid Tokens |
| | CAPCOM | Street Fighters |
| | ATARI | Atari Token |

출처) Nonfungible.com, KOTRA 실리콘밸리 무역관 정리 내용 재구성

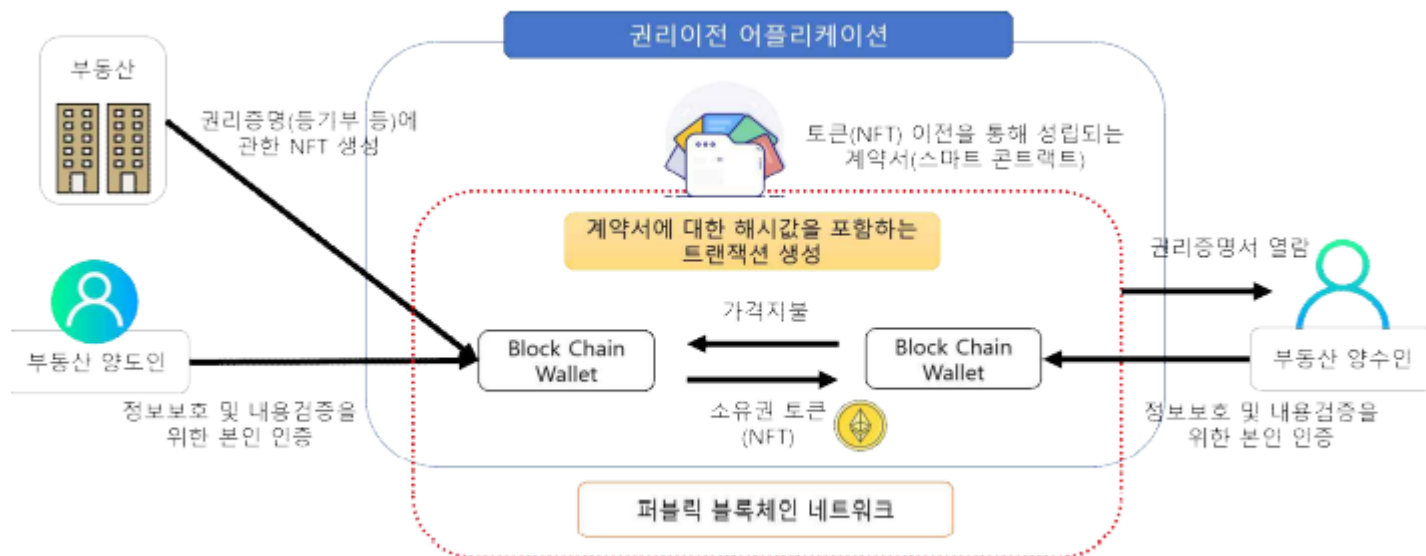
➔ Non-Fungible Token (NFT)

□ NFT 현황 및 활용 사례

▣ NFT를 통한 부동산과 자동차 등 거래 시스템 실증

- 퍼블릭 블록체인 기반으로 부동산의 권리 이전 이력관리, 계약서 및 부동산 정보, 계약 내용 등을 열람(참여자 인증 필수) 할 수 있도록 시스템 구축

〈 일본 부동산 NFT 거래 프로세스(실증안) 〉



출처) <https://crypto.watch.impress.co.jp/docs/news/1215138.html> 재구성

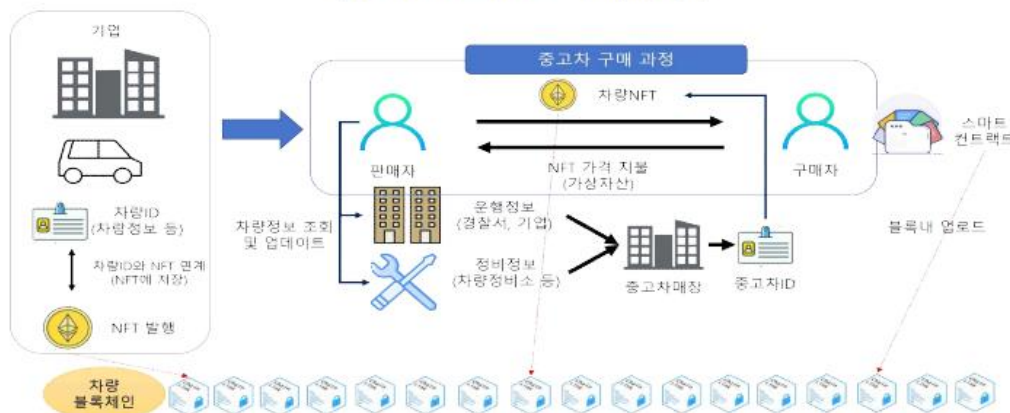
➔ Non-Fungible Token (NFT)

□ NFT 현황 및 활용 사례

▣ 일본 중고차 거래시장을 대상으로 NFT 활용 검증 (2020)

- 일본 자동차회사 도요타와 블록체인 기업 Datachain이 협업
 - 교통법규 위반 사항, 자동차 제조이력, 정비 이력 등을 기관으로부터 수집하여 차량에 대한 NFT 발행
 - 실물 차량과 차량 NFT에 대한 대금을 가상자산으로 지불하는 "온라인 직거래" 시스템을 구현

〈 중고차 NFT 거래 프로세스(실증안) 〉

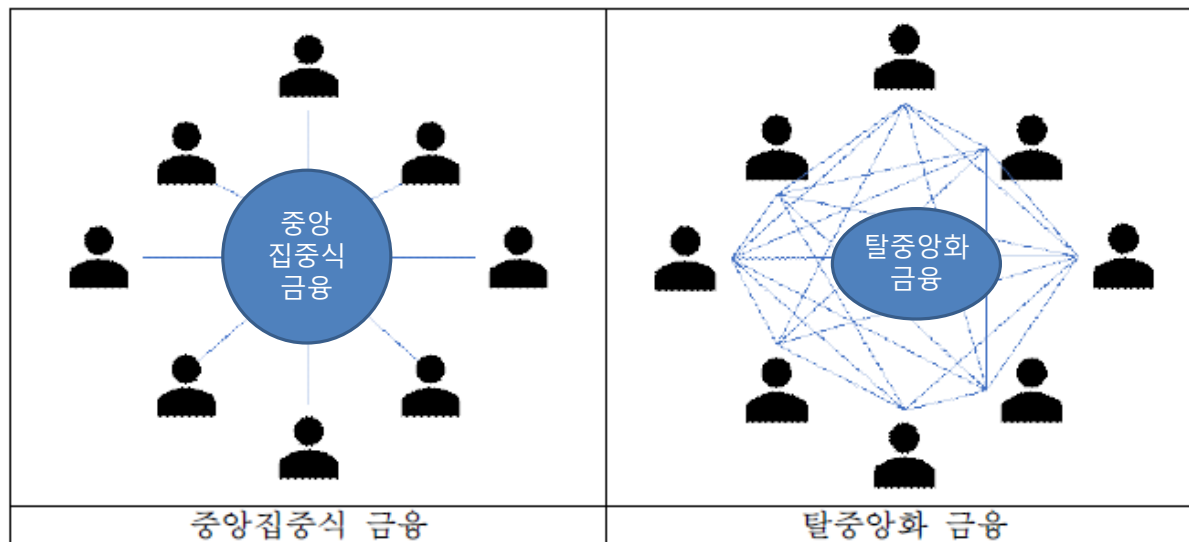


출처) <https://hedge.guide/news/blockchain-poc-bc202003.html> 재구성

Decentralized Finance (DeFi)

□ DeFi

- ▣ 탈중앙화 금융으로, 분산 금융 또는 분산 재정 의미
- ▣ 암호화폐를 담보로 걸고 일정 금액을 대출 받거나, 다른 담보를 제공하고 암호화폐를 대출 받는 방식으로 작동



Decentralized Finance (DeFi)

□ DeFi

▣ DeFi 기술 필수 요소

- 탈중앙화 메인넷
 - 블록체인을 위한 필수적인 메인 네트워크(e.g., 이더리움)
- 스마트 컨트랙트 코드
 - 투명한 스마트 컨트랙트 코드 공개를 통한 금융 로직을 확인이 가능하며, 이자율, 배분 조건 등과 같은 '계약'(Contracts) 내용들을 공개
 - 정상적으로 잘 작동할 경우, 금융 자동 로직에 외부 개입이 불가능함
 - 임의의 행위로 인해 작동 중단이 불가능함(검열저항성)
 - 국가 규제기관의 허락 없이 글로벌 금융 서비스 제공이 가능
- 지갑 (Wallet)
 - 사용자들의 접근이 쉽도록 가상자산을 저장할 수 있는 익히기 쉬운 가상자산 지갑이 필요

□ DeFi

▣ DeFi 기술 필수 요소

- 거버넌스 장치

- 추가 발행이나 소각과 같은 가상자산 관련 정책 변경, 블록체인의 상의 정책이나 코드 수정, 오류 대응을 위한 코드 업데이트를 위한 의사결정과 집행을 위한 특수 권한을 작동시킬 수 있는 장치

- 탈중앙화 거래소

- 거래 내역 전체를 관리하고 책임지는 중앙 기관없이 코드화된 룰로써, 스마트계약에 기반을 두어 비인격적으로 자동하는 거래소
- 중앙화된 가상자산 거래소를 거치지 않고, 서로 다른 코인을 직접 교환할 수 있는 트레이딩들이 적용되는 거래소

Decentralized Finance (DeFi)

□ DeFi

▣ 기존 금융과 DeFi의 차이

| 구분 | 기존 금융 | De-Fi |
|----------|-----------------------|--------------------------|
| 허가 | 특정 고객 | 네트워크상 존재하는 모든 고객 |
| 운영 주체 | 중앙화 | 탈중앙화 |
| 중개인 | 신뢰 기관 필요 | 네트워크 참여자가 대체 |
| 투명성 | 특정 사용자만 접근 가능 | 모든 사용자가 거래 기록을 공유 |
| 검열 방지 | 검열 기관에 의해 특정 거래 삭제 가능 | 하나의 주체가 특정 거래 기록 무효화 불가능 |
| 프로그래밍 가능 | 독점 소프트웨어로 한정된 프로그래밍 | 오픈 소스를 통한 자유로운 프로그래밍 |

출처: 헤슬란트(Hexlant Research)

Decentralized Finance (DeFi)

□ DeFi

- ▣ DeFi는 블록 체인에서 금융 기능을 수행하는 DApp (분산 형 애플리케이션)으로 알려진 애플리케이션을 중심으로 전개됨
- ▣ DeFi 프로토콜은 자산에 대한 순간적 수요에 따라 이자율을 자동으로 조정함
- ▣ 이더리움 블록 체인에서 실행

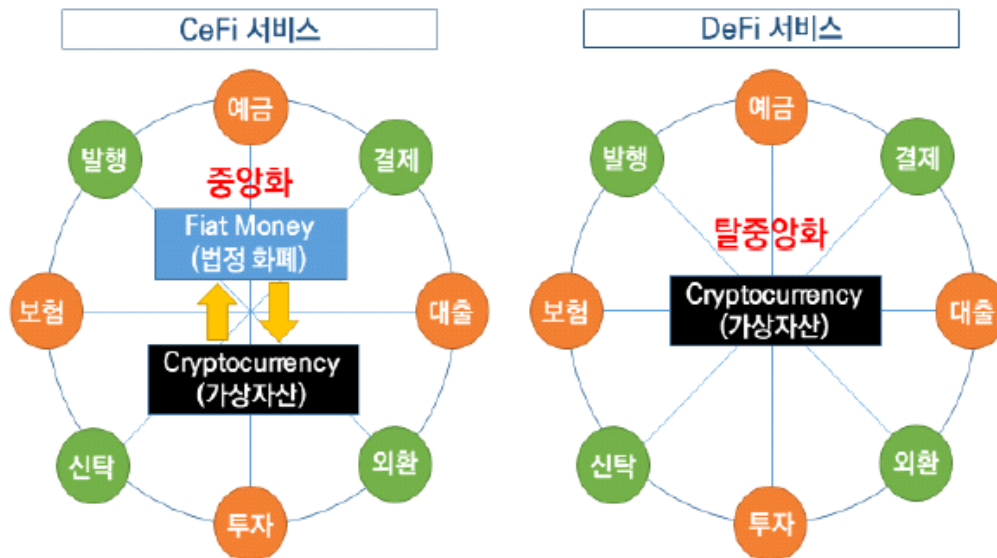
Decentralized Finance (DeFi)

□ DeFi

- ▣ 블록체인 네트워크상에서 스마트 컨트랙트를 활용하여 동작하는 탈중앙화 금융 서비스
 - 가상자산(Cryptocurrency)을 기반으로 금융 서비스를 수행

□ Centralized Finance (CeFi)

- ▣ 중앙화 금융 (e.g., 가상자산 거래소 - 바이낸스, 업비트)



Decentralized Finance (DeFi)

□ 디파이와 다른 금융 간의 차이점

| 구분 | 디파이 | 씨파이 | 전통금융 | 핀테크 |
|---------------|---|------------------------------|--|---------------------------------|
| 이용 화폐 | 가상자산 | 가상자산, 법정화폐 | 법정화폐 | 법정화폐 |
| 중개자 및 관리주체 | 블록체인 네트워크 (거버넌스 토큰) | 가상자산 거래소 | 전통금융기관 | 핀테크업체 |
| 이용 화폐의 보관 | 지갑 | 가상자산 거래소 | 전통금융기관 | 전통금융기관 |
| 금융서비스 | 예금, 대출, 가상자산 거래, 파생상품, 자산관리, 결제, 보험 등 | 가상자산 거래, 대출 | 예금, 대출, 증권거래, 환전, 파생상품, 자산관리, 결제, 보험 등 | 결제, 대출, 투자, 보험 |
| 익명성 | 익명 거래 | 실명 거래 | 실명 거래 | 실명 거래 |
| 투명성 | 투명 | 불투명 | 불투명 | 불투명 |
| 국가 간 경계 | 없음 | 있음 | 있음 | 있음 |
| 기업 사례 | 메이커, 에이브, 유니스왑, 컴파운드, 신세틱스 등 | 바이낸스, 코인베이스, 빗썸, 업비트 등 | JP모건, 골드만삭스, 뱅크오브아메리카, HSBC 등 | 엔트파이낸셜, 스트라이프, 로빈후드, 토스 등 |

자료: KAIST(2020), 김협 외(2021), 저자 재구성

□ 이더리움 오라클

- 'Oracle'은 이더리움 외부에서 일어나는 문제들에 대한 정보를 알려주는 시스템
 - 즉, 외부의 데이터를 스마트 컨트랙트로 제공하는 시스템이며 신뢰가 필요없는 시스템



□ 오라클 필요성

- 이더리움 플랫폼의 핵심은 컨센서스 규칙에 의해 프로그램을 실행하고 상태를 업데이트하는 EVM (Ethereum Virtual Machine)임
 - 컨센서스를 유지하기 위해서 EVM은 항상 결정적으로만 실행되어야 함
 - 이더리움 상태와 트랜잭션의 컨텍스트에 기반을 두어야함
- ⇒ 1. EVM 및 스마트 컨트랙트와 같이 동작하는 임의성을 위한 고유한 소스가 없음
- ⇒ 2. 외부 데이터가 트랜잭션의 페이로드로만 유입 됨

□ 오라클 필요성

■ EVM 및 스마트 컨트랙트와 같이 동작하는 임의성을 위한 고유한 소스가 없음

- EVM에서 컨트랙트에 임의성을 제공하기 위한 난수 함수를 사용하게 될 경우, 같은 코드를 실행하고 결과가 다른, 즉 합의가 되지않는 상황이 나오게 될 수 있음

- 예) **노드 A**는 특정 스마트 컨트랙트 '**SC**'의 명령어를 실행하고 스토리지에 **3**을 저장, **노드 B**는 동일한 스마트 컨트랙트 '**SC**'를 실행하고 **7**을 저장

- **노드 A**와 **노드 B**가 동일한 컨텍스트에서 정확하게 동일한 코드를 실행했음에도 결과 상태가 다르게 나옴

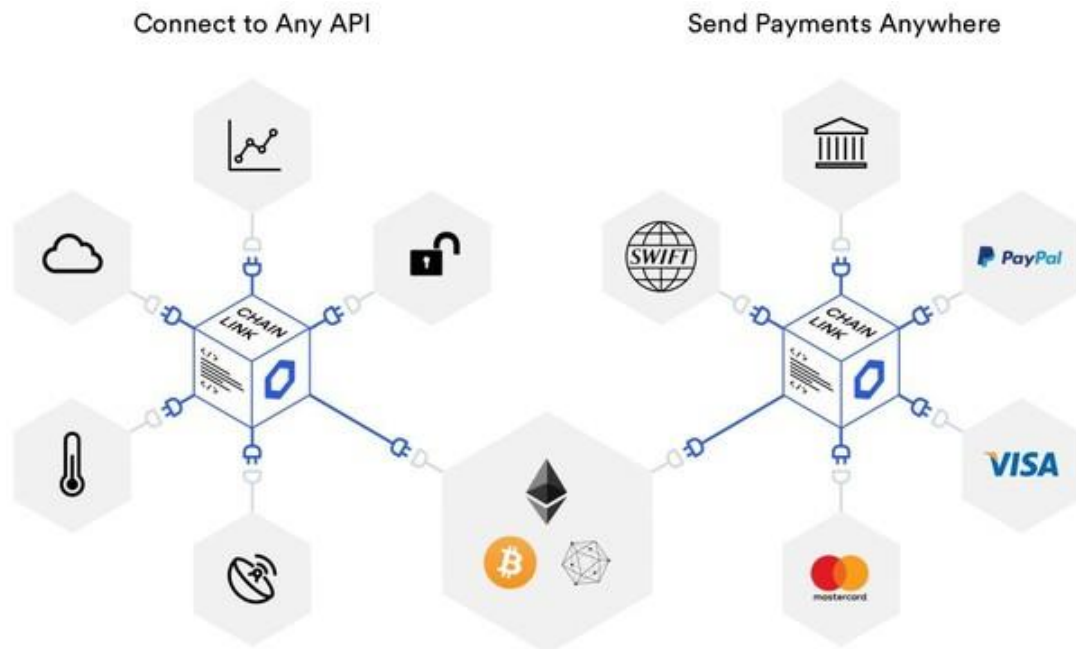
- 즉, **스마트 컨트랙트가 실행될 때마다 다른 결과 상태가 나올 수 있음 => 탈중앙화된 합의가 불가능하게 될 수 있음**

□ 오라클 필요성

- EVM 및 스마트 컨트랙트와 같이 동작하는 임의성을 위한 고유한 소스가 없음
 - 일반적으로 암호화된 보안 해시함수와 같은 의사 난수 함수 (pseudorandom function)들은 다양한 애플리케이션에서 사용하기에 충분하지 못함

□ 오라클 사례

- 오라클은 이상적으로 스마트 컨트랙트를 위해 이더리움 플랫폼으로 축구 경기의 결과, 금 가격, 순수 난수 등의 외부(실세계 혹은 오프체인) 정보를 가지고 오는 데 있어서 신뢰가 필요 없는(trustless or near-trustless) 방법을 제공함



□ 오라클 사례

- 양자/열처리와 같은 물리적인 소스로부터 발생하는 난수/엔트로피
- 자연재해에 대한 파라미터 트리거: 지진 규모 측정
- 환율 데이터: 법정 화폐에 대한 암호화폐 교환 비율
- 자본 시장 데이터: 토큰화된 자산/증권의 가격 책정
- 시간 및 간격 데이터: 정확한 시간 측정에 근거한 이벤트 트리거
- 날씨 데이터: 일기예보에 기초한 보험료 계산
- 지리적 위치 데이터: 공급망 추적에 사용되는 데이터
- 등등

□ 오라클 디자인 패턴

▣ 모든 오라클의 핵심 기능

- 오프체인 소스에서 데이터를 수집
- 해당 데이터를 서명된 트랜잭션으로 온체인에 전송
- 데이터를 스마트 컨트랙트의 저장소에 저장하여 사용할 수 있게 함

▣ 오라클 설정을 위한 주요 3개 방법

- 즉시 읽기 (immediate-read)
- 게시-구독 (publish-subscribe)
- 요청-응답 (request-response)

□ 오라클 디자인 패턴

▣ 오라클 설정을 위한 주요 3개 방법

- 즉시 읽기 (immediate-read)

- 즉각적인 결정에 필요한 데이터를 제공
- '즉시 읽기' 유형의 오라클은 데이터 요청에 응답하기 위해 서버를 운영하고 유지관리해야 하는 조직이나 회사에서 사용하기 좋을 수 있음
 - 변경되지 않는 정보를 저장해 놓고 읽기만 하는 방식
 - 오라클에 의해 저장된 데이터는 효율성이나 프라이버시 때문에 오라클이 제공하는 raw 데이터가 아닐 가능성이 높음 (개인정보 비식별화를 통한 데이터일 경우)

□ 오라클 디자인 패턴

▣ 오라클 설정을 위한 주요 3개 방법

– 게시-구독 (publish-subscribe)

- '게시-구독' 형태의 오라클은 예서정기적 혹은 잦은 변화가 예상되는 데이터를 효과적으로 브로드 캐스트하는 역할
- 데이터는 온체인 스마트 컨트랙트에 의해 폴링(polling)되거나 업데이트를 위한 오프체인 데몬에 의해 모니터링됨
- 오라클은 새로운 정보로 업데이트되고, 플래그는 새로운 데이터를 사용할 수 있음을 '구독' 대상들에게 알리는 방식
 - 가격 정보, 기상 정보, 경제 또는 사회 통계, 교통 정보 등이 있음

□ 오라클 디자인 패턴

■ 오라클 설정을 위한 주요 3개 방법

- 요청-응답 (request-response)

- 스마트 컨트랙트에 저장하기에 데이터가 너무 크고, 사용자는 전체 데이터 중 일부만 필요로 한 경우에 사용됨
 - 데이터 공급자 사업 영역에 적용 가능한 모델
- 오라클은 요청을 모니터링하면서 데이터를 검색 및 반환하는데 사용되는 온체인 스마트 컨트랙트와 오프체인 인프라 시스템으로 구현될 수 있음
 - 1. 댕(Dapp)으로부터 질의(Query)를 받음
 - 2. 질의(Query)를 분석
 - 3. 비용 지불 및 데이터에 접근 권한 확인
 - 4. 오프체인 소스에서 관련 데이터를 검색
 - 5. 데이터가 포함된 트랜잭션에 서명
 - 6. 트랜잭션을 네트워크로 브로드캐스트
 - 7. 알림 등 필요한 추가 트랜잭션을 스케줄링함

□ 데이터 인증

- ▣ 데이터 소스에 대한 신뢰성이 있다고 가정할 경우, 데이터를 온체인으로 올리는 주체는 신뢰할 수 없음
- ▣ 오라클의 메커니즘을 무한정 신뢰할 수 없고 전송 중에 데이터가 변조될 수 있으므로 데이터의 무결성을 입증할 수 있는 오프체인 방식의 검증 방법이 필요
- ▣ 데이터 인증의 두가지 접근 방법
 - '진위성 증명 (Authenticity proof)'과 '신뢰할 수 있는 실행 환경 (Trusted Execution Environment, TEE)'

□ 데이터 인증

▣ 진위성 증명 (Authenticity proof)

- 스마트 컨트랙트는 체인상의 진위성 증명을 검증함으로써 데이터를 처리하기 전에 데이터의 무결성을 검증함
- 즉, 데이터가 변조되지 않았음을 암호학적으로 보증
 - 오라클라이즈(Oraclize, <https://provable.xyz/>)
 - 클라이언트 서버간에 HTTPS 웹 트래픽이 발생했다는 증거를 제 3자에게 제공할 수 있는 TLSNotary 증명

▣ 신뢰할 수 있는 실행 환경 (TEE)

- 데이터 무결성을 보장하기 위해 하드웨어 기반의 고립된 보안 영역 (enclave)을 사용
 - 타운 크리에 (Town Crier, <http://www.town-crier.org/>)는 TEE 접근 방식에 기반한 인증된 오라클 시스템 (Intel SGX 사용)

□ 계산 오라클

- ▣ 데이터 요청 및 전달 이외에 임의의 계산을 수행할 수 있음
 - 예: 채권 컨트랙트의 수익률 추정

□ 탈중앙화 오라클

- ▣ 중앙화된 데이터 또는 계산 오라클의 경우, 이더리움 네트워크에서 단일 실패 지점 (Single Point Of Failure, SPOF)이 될 수 있음
 - 단일 실패 지점: 시스템 구성 요소 중에서 동작이 안될 경우, 전체 시스템 마비 또는 중단되는 요소

- ❑ 오라클은 스마트 컨트랙트에 중요한 서비스를 제공하며 스마트 컨트랙트 실행을 위해 외부에서 특정 데이터를 가져옴
- ❑ 오라클 서비스를 제공 주체가 직접 데이터 소스를 제공할 경우 심각한 문제가 발생할 수 있음
 - 오라클을 사용해야 할 경우 신뢰 모델에 대해 신중하게 고려해야함
 - 잘못된 입력에 노출되어 스마트 컨트랙트의 보안을 약화시킬 수 있음

- ❑ “블록체인 기반 혁신금융 생태계 연구보고서”, 한국인터넷진흥원
- ❑ “NFT 기술의 이해와 활용, 한계점 분석”, 한국인터넷진흥원

Q & A

