



# 목차



- 토큰 스마트컨트랙트
  - ERC-20: 대체 가능 토큰(Fungible Token) 표준
  - ERC-721: 대체 불가능 토큰(Non-Fungible Token, NFT) 표준

# **EIP(Ethereum Improvement Proposal)**



- EIP(Ethereum Improvement Proposal: 이더리움 개선 제안)
  - 이더리움 네트워크에 대한 변경 제안을 설명하는 문서
  - 핵심 프로토콜 사양, 클라이언트 API 및 계약 표준을 포함하여 Ethereum 플랫
     폼에 대한 표준을 설명
  - 이더리움 생태계의 발전과 업그레이드를 위해 개발자 및 이용자 커뮤니티에
     의해 작성되고 검토됨
  - 합의가 이루어진 EIP는 이후 이더리움 업그레이드에서 반영되어 전체 네트워 크에 적용
  - 예
    - EIP-1559: 거래 수수료 메커니즘 변경(Base Fee 도입), 2021년 런던 하드포크
    - EIP-55: 주소에 체크섬을 추가하여 주소의 무결성을 검증하고 오류로부터 보호

## **ERC(Ethereum Request for Comments)**



### ERC(Ethereum Request for Comments)

- EIP 중 스마트컨트랙트 표준에 관련된 제안이 커뮤니티에서 채택되면 ERC
- 이더리움 기반 블록체인에서 토큰을 발행하고 관리하기 위한 핵심 규칙
- 이더리움 생태계에서 표준화된 규격을 제안하고 논의하기 위한 문서
- 주로 스마트 컨트랙트, 토큰 및 다양한 기능을 정의하며, 이를 통해 이더리움
   생태계에서의 일관성과 상호 운용성을 향상시키기 위해 사용
- ERC-20, ERC-721, ERC-1155 등



## ERC-20(Ethereum Request for Comment 20)

- https://eips.ethereum.org/EIPS/eip-20
- 이더리움 블록체인 네트워크의 표준 토큰 스마트 컨트랙트
- 이더리움 네트워크에서 가장 많이 사용되는 토큰 그룹
- 화폐처럼 계정(Account)들 간의 거래에 사용
- 이더리움 네트워크에 배포된 대체 가능 토큰(Fungible Token) 표준
  - Alice가 들고 있는 100원 = Bob이 들고 있는 100원
  - Alice가 들고 있는 1개의 토큰 = Bob이 들고 있는 1개의 토큰
- 대부분의 이더리움 기반 암호화폐가 ERC-20을 따름
- 사용 사례: ICO(Initial Coin Offering)



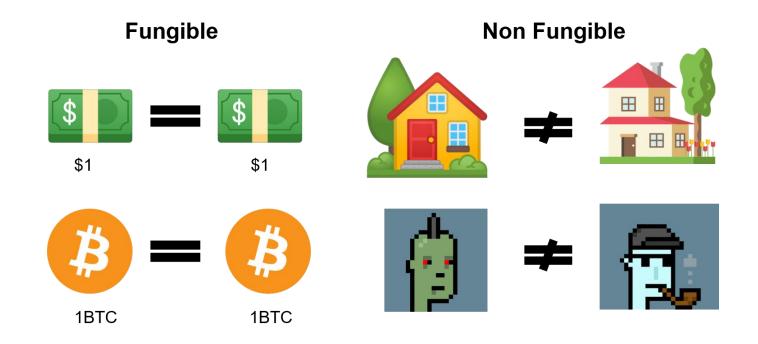
- NFT(Non-Fungible Token)를 발행하기 위한 표준
- 대체 불가능한 토큰(NFT)
  - 블록체인에 기록되는 고유한 디지털 식별자로 소유권과 진위 여부를 인증하는 데 사용
  - 복사, 대체, 분할 불가능
  - NFT의 소유권은 블록체인에 기록되며 소유자가 양도할 수 있으므로 NFT를 판매 및 거래 가능
  - 일반적으로 예술 작품, 사진, 비디오 및 오디오와 같은 디지털 파일에 대한 참조가 포함됨
  - 블록체인 고양이 게임인 크립토키티에서 각각의 고양이는 모두 독특한 특성이 있어서 다른 고양이로 대체하는 것이 불가능(고유성과 희소성)

# Fungible과 Non Fungible



## ■ Fungible과 Non Fungible

- 대체 가능(fungible)한 토큰: 각기 동일한 가치를 지녀 서로 교환이 가능, 이에 해당하는 것이 명목화폐, 암호화폐, 채권 등
- 대체불가토큰: 하나의 토큰을 다른 토큰으로 대체하는 것이 불가능한 암호화폐







- 2016년 크립토 키티
  - 사용자들이 가상의 고양이를 사고, 모으고, 기르고 팔 수 있는 이더리움 블록체인상
     의 NFT 프로젝트
  - 256비트의 유전자 정보를 NFT 메타데이터, 교배(Breeding) 시스템을 활용
  - 이더리움 네트워크를 마비시킬 정도의 파급력을 가졌음. 런칭 후 1,200만 달러 투자
- 2017년 크립토 펑크
  - 남자, 여자, 좀비, 유인원, 외계인 / 5개 캐릭터로 구성된 캐릭터 NFT
  - 2017년 출시 당시 9,000개 무료 제공
  - "최초의" 한정판 NFT -> 현재 3억~ 최대 1400억
  - 24x24 8bit 픽셀 아바타





- 2021년 Bored Ape Yacht Club
  - 수집품 이상의 가치를 가진 NFT가 각광받기 시작하는 계기
  - BAYC NFT 소유자가 특별한 커뮤니티와 혜택에 접근할 수 있는 디지털 멤버십



- NFT 활용
  - NFT를 활용한 커뮤니티 구축
  - 멤버십, 입장권, 프라이빗 클럽 등 소유자의 로열티를 끌어올리는 각종 장치
  - 저작권 관리, 예술작품, 게임, 메타버스 등



- ERC-1155: 멀티 토큰 표준(Fungible + Non-Fungible)
  - ERC-721의 개념을 확장
  - 하나의 컨트랙트에서 대체가능 토큰과 대체불가능 토큰을 동시에 생성하고 관리
  - 많은 양의 토큰을 한 번에 관리: 토큰 배치 전송(batch transfer) → 거래 비용과 시간을 절약
  - 사례: 2022년 12월에 출시된 '아디다스 인투 더 메타버스(Adidas Into the Metaverse)' 컬렉션
    - 디지털 스니커즈, 의류 등 다양한 디지털 자산을 포함
    - 디지털 스니커즈 같은 대체 가능한 토큰(Fungible Token)과 가상 부동산과 같은 대체 불가능한 토큰(Non-Fungible Token)을 한 스마트 계약 안에서 동시에 생성하고 관리
    - 디지털 스니커즈와 의류 등을 한 번에 구매하면서 거래 비용과 시간을 절약할 수 있다
       는 장점



- ERC-20
  - 이더리움 창시자 V. Buterin 처음 제안



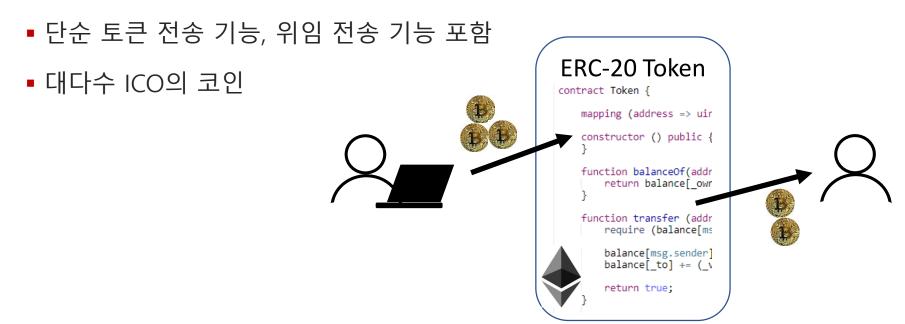
"사용자와 응용프로그램들이 서로 쉽게 토큰을 주고받을 수 있도록 공통 사용사례를 표준화할 필요가 있다."

"Although Ethereum allows developers to create absolutely any kind of application without restriction to specific feature types, there is nevertheless a need to standardize certain very common use cases in order to allow users and applications to more easily interact with each other."

- V. Buterin, EIP 20: ERC-20 token standard, 2015.

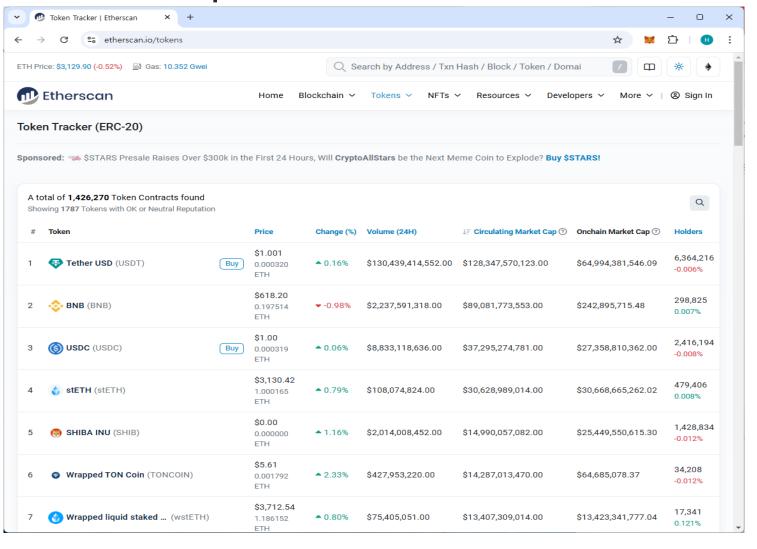


- 이더리움 블록체인에서 사용하는 토큰들의 호환을 위한 표준 명세
- 토큰: 이더리움 스마트컨트랙트의 대부분을 차지
- 다양한 토큰들을 하나의 응용프로그램에서 관리 가능
  - 예: 월렛(Wallet), 분산 거래소(Decentralized exchanges)



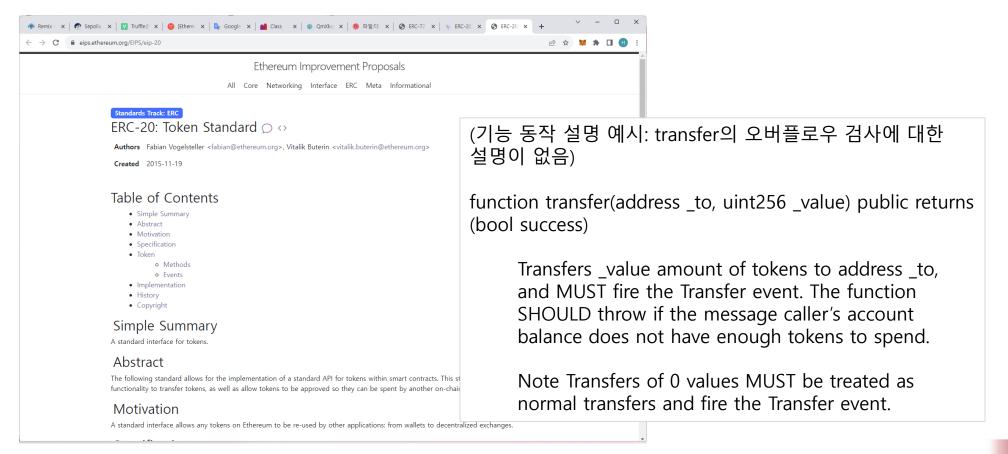


■ 이더스캔: ERC-20 Top Tokens





- 표준 내용
  - 함수 이름, 인자와 타입, 리턴 타입(API)만 정의
  - 동작에 대한 불완전한 설명(예: transfer의 오버플로우)





# • 6개 필수 함수 API + 2개 이벤트

Methods	
name	function name() public view returns (string)
symbol	function symbol() public view returns (string)
decimals	function decimals() public view returns (uint8)
totalSupply	function totalSupply() public view returns (uint256)
balanceOf	function balanceOf(address _owner) public view returns (uint256 balance)
transfer	function transfer(address _to, uint256 _value) public returns (bool success)
transferFrom	function transferFrom(address _from, address _to, uint256 _value) public returns (bool success)
approve	function approve(address _spender, uint256 _value) public returns (bool success)
allowance	function allowance(address _owner, address _spender) public view returns (uint256 remaining)
Events	
Transfer	event Transfer(address indexed _from, address indexed _to, uint256 _value)
Approval	event Approval(address indexed _owner, address indexed _spender, uint256 _value)



### ■ ERC-20 필수 함수

- totalSupply()
  - 발행한 총 토큰 수를 반환
- balanceOf(address \_owner)
  - \_owner가 소유한 토큰 수를 반환
- transfer(address \_to, uint256 \_value)
  - 발신자(msg.sender)로부터 받는 계정 주소(\_to)로 \_value만큼의 토큰을 전송
  - 사용자에게 전송 성공 여부를 알리기 위해 bool 유형의 결과값을 반환
  - Transfer 이벤트 발생 : 세 가지 값을 갖는 이벤트
    - 보낸 계정 주소(from), 받는 계정 주소(to), 전송 된 토큰 수(value)
  - 보내는 계정의 잔액이 \_value보다 작으면 throw
  - 0(zero) 전송도 일반적인 전송으로 처리



### ■ ERC-20 필수 함수

- transferFrom(address \_from, address \_to, uint256 \_value)
  - 보내는 계정(from)에서 받는 계정(to)으로 value만큼의 토큰을 발신자가 위임 전송
  - 사용자에게 전송 성공 여부를 알리기 위해 bool 유형의 결과값을 반환
  - Transfer 이벤트 발생 : 세 가지 값을 갖는 이벤트
    - 보낸 계정 주소(from), 받는 계정 주소(to), 전송 된 토큰 수(value)
  - 보내는 계정의 잔액이 \_value보다 작으면 throw
  - 0(zero) 전송도 일반적인 전송으로 처리
  - 보내는 계정으로부터 발신자가 위임 받은 금액이 value보다 작으면 throw



#### ■ ERC-20 필수 함수

- approve(address \_spender, uint256 \_value)
  - 토큰 소유자(발신자, msg.sender)가 자신의 토큰을 \_value 만큼 인출할 수 있는 권한을 \_spender 에게 위임
  - 성공 여부를 알리기 위해 bool 유형의 결과값을 반환
  - Approval 이벤트 발생
    - 토큰 소유자 계정(owner), 대리 인출자 계정(spender), 승인한 토큰 수(value)
- allowance(address \_owner, address \_spender)
  - \_spender가 \_owner로부터 대리 인출할 수 있는 토큰 수를 반환



### ■ ERC-20 토큰 스마트 컨트랙트 개발 실습: ERC20StdToken

```
각 계정이 소유한
                                                                                토큰 수 저장
contract ERC20StdToken {
 mapping (address => uint256) balances;
                                                                       각 계정이 다른 계정들이
 mapping (address => mapping (address => uint256)) allowed;
                                                                       대리 전송할 수 있도록
                                                                       허용한 토큰 수 저장
 uint256 private total;
 string public name;
 string public symbol;
                                                                                총 발행 토큰 수
 uint8 public decimals;
                                                                           토큰 이름
                                                                           토큰 심볼
 event Transfer(address indexed from, address indexed to, uint256 value);
                                                                           토큰의 소수점 자리수
 event Approval(address indexed owner, address indexed spender, uint256 value);
```



## ■ ERC-20 토큰 스마트 컨트랙트 개발 실습: ERC20StdToken

```
constructor (string memory name, string memory symbol, uint totalSupply) {
     total = _totalSupply;
     name = name;
     symbol = _symbol;
     decimals = 0;
     balances[msg.sender] = totalSupply;
     emit Transfer(address(0x0), msg.sender, _totalSupply);
function totalSupply() public view returns (uint256) {
function balanceOf(address owner) public view returns (uint256 balance) {
function allowance(address owner, address spender) public view returns (uint256 remaining) {
```



## ■ ERC-20 토큰 스마트 컨트랙트 개발 실습: ERC20StdToken

function transfer(address \_to, uint256 \_value) public returns (bool success) {



■ ERC-20 토큰 스마트 컨트랙트 개발 실습: ERC20StdToken

function transferFrom(address \_from, address \_to, uint256 \_value) public returns (bool success) {

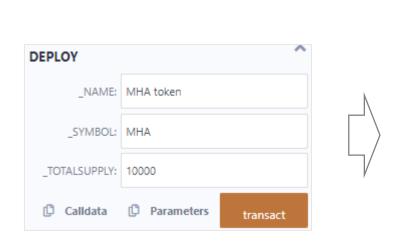


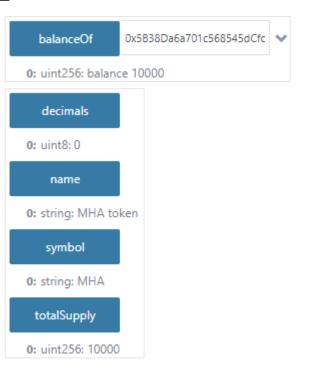
■ ERC-20 토큰 스마트 컨트랙트 개발 실습: ERC20StdToken

```
function approve(address _spender, uint256 _value) public returns (bool success) {
}
```



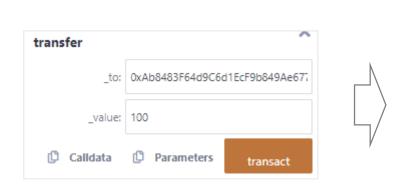
- 테스트
  - 배포: 이름,심볼,총 토큰수
    - 배포 직후에는 모든 토큰을 배포자가 가지고 있음







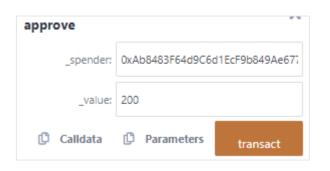
- 테스트
  - transfer 테스트
    - 컨트랙트소유자(배포자,Account1)로부터 새로운 계정으로 토큰 전송





## ■ 테스트

- approve 테스트
  - approve 함수로 컨트랙트소유자(Account1)로부터 다른 계정(Account2)으로 위임
  - allowance함수로 위임 확인





```
"event ": "Approval",
"args": {
    "0": "0x5B38Da6a701c568545dCf cB03FcB875f 56beddC4",
    "1": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
    "2": "200",
    "owner ": "0x5B38Da6a701c568545dCf cB03FcB875f 56beddC4",
    "spender ": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
    "value": "200"
}

allowance

_owner: 0x5B38Da6a701c568545dCfcB03FcBi
_spender: 0xAb8483F64d9C6d1EcF9b849Ae677

Calldata Parameters call

0: uint256: remaining 200
```



### ■ 테스트

■ transferFrom 테스트

• 위임받은 계정(Account2)가 컨트랙트소유자(Account1)로부터 또다른 계정

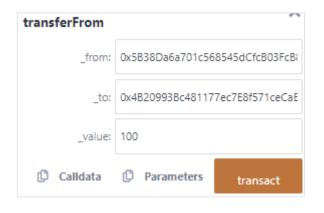
"event": "Transfer",

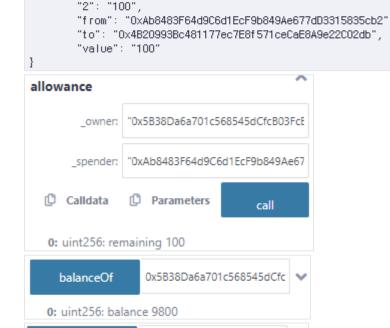
balanceOf

0: uint256: balance 100

"args": {

(Account3)으로 위임전송



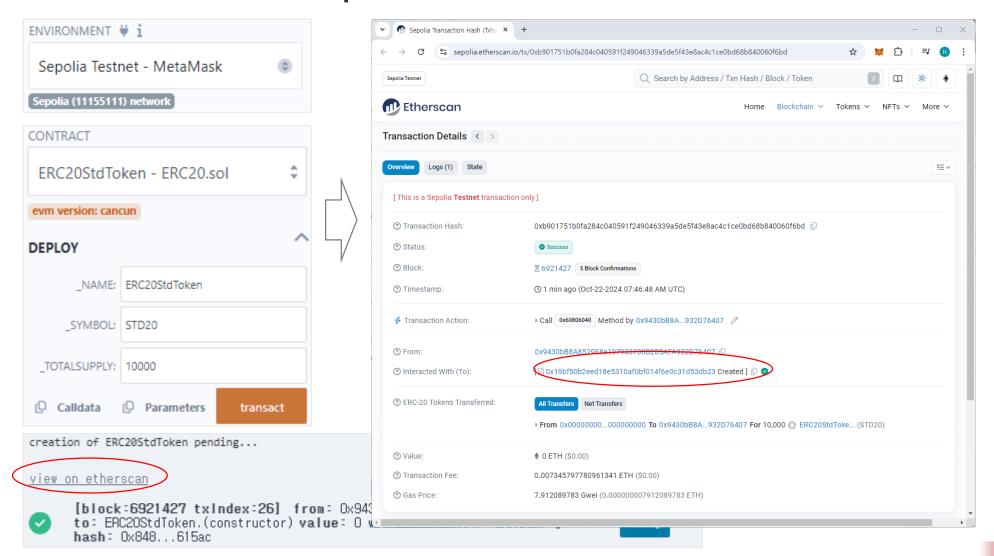


0x4B20993Bc481177ec7E8f5: >

"0": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2", 
"1": "0x4B20993Bc481177ec7E8f571ceCaE8A9e22C02db",



■ 테스트: remix에서 Sepolia 테스트 네트워크에 배포



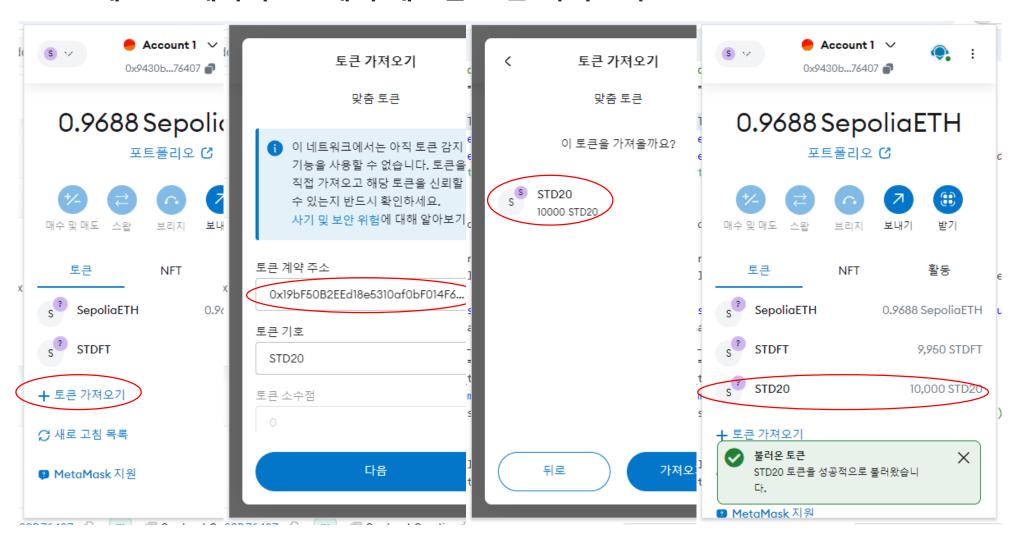


■ 테스트: 메타마스크 Sepolia 계정



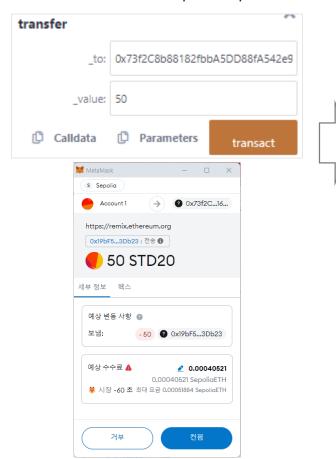


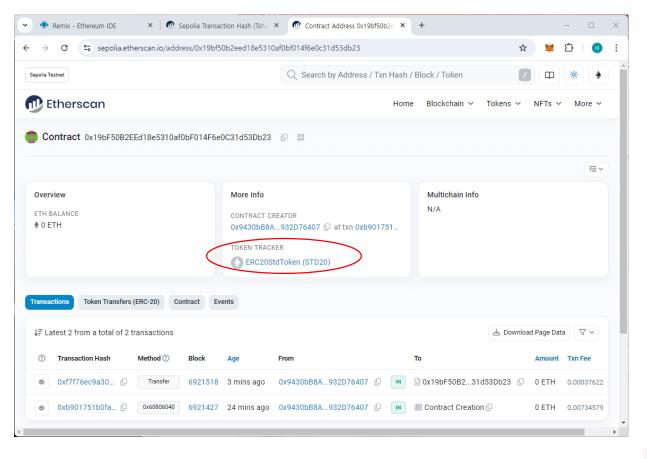
■ 테스트: 메타마스크에서 배포한 토큰 가져오기





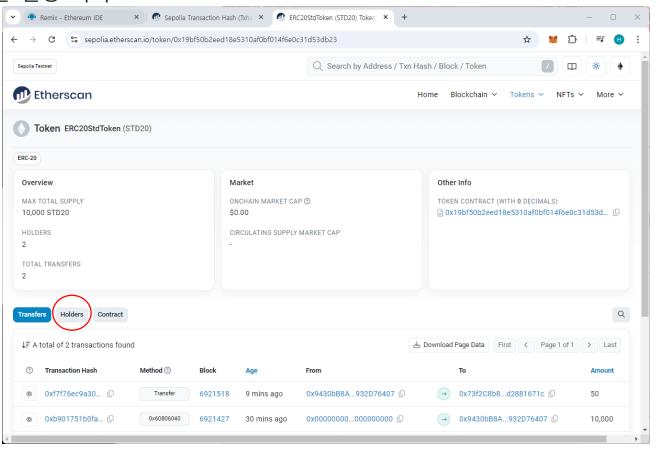
- 테스트: remix에서 Sepolia 테스트 네트워크에 배포한 토큰 전송
  - 토큰전송후 이더스캔 컨트랙트 정보 화면
    - https://sepolia.etherscan.io/address/0x19bf50b2eed18e5310af0bf014f6e0c31d53db23





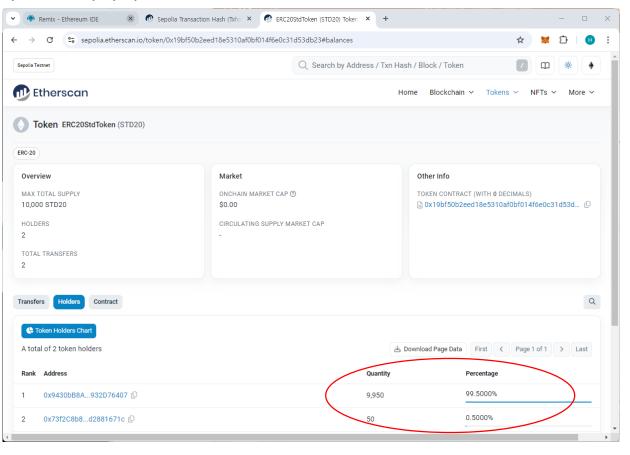


- 테스트: Sepolia 테스트 네트워크에 배포 후 토큰 전송
  - 이더스캔 [More Info] -> [TOKENTRACKER]
    - 토큰 전송 기록





- 테스트: Sepolia 테스트 네트워크에 배포 후 토큰 전송
  - 이더스캔 [More Info] -> [TOKENTRACKER] -> [Holders]
    - 소유자 정보 페이지





#### • ERC-721 NFT 표준

- 이더리움 기반의 블록체인에서 NFT(Non-Fungible Token)를 생성하고 관리할 수 있는 토큰 표준
  - 토큰 표준(Token Standard): 블록체인에서 스마트 계약(smart contract)을 이용해 발행되는 토큰들이 공통적으로 지켜야 하는 규칙
- 2017년 크립토키티(CryptoKitties)라는 가상 고양이 컬렉션 게임이 선풍적인 인기를 끌면서 널리 알려짐
  - ERC-721 토큰을 사용해 사용자가 소유한 각각의 고양이를 구별하고, 소유권을 증명
- 디지털 자산의 소유권을 명확히 증명하고, 이를 안전하게 거래하고자 하는 목
   적에서 시작
- 디지털 아트, 가상 부동산, 온라인 게임 아이템, 디지털 아트, 게임 아이템, 블록체인 기반의 투표 시스템 등 다양한 분야에서 널리 활용



#### • ERC-721 NFT 표준

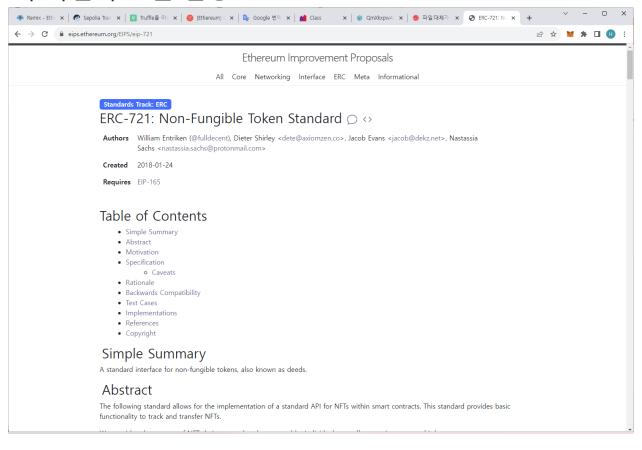
- 가장 큰 특징은 고유한 속성과 식별자(ID)를 가지고 있다는 점 → 다른 토큰으로 대체가 불가능
- 개별 토큰의 소유권과 전송 기록이 모두 블록체인에 저장되기 때문에 투명하 게 거래할 수 있음
- 스마트 계약을 통해 발행하고 관리되어 중앙화된 관리 주체 없이 신속하고 안 전하게 거래될 수 있음



- NFT의 정보와 소유자, 거래 내역 등의 메타데이터는 모두 블록체인상에 저장
- NFT의 원본 데이터 저장: IPFS(InterPlanetary File System, 분산형 파일 시스템)
  - IPFS: 인터넷상에서 파일을 분산 저장하고 공유하기 위한 서버
    - 저장공간이 해킹 당하거나 데이터가 삭제되면 NFT 가치가 심하게 훼손되기 때문에, 원본 데이터 저장과 백업을 위해 IPFS 분산 네트워크를 사용
    - 대표적인 NFT 마켓 플레이스인 오픈씨(OpenSea)와 라리블(Rarible)
  - NFT 내에 원본 파일까지 함께 저장할 수 있지만, 데이터의 크기가 커져 거래에 있어 과도한 수수료(가스비)가 발생
  - NFT 아티스트 비플(Beeple)의 '매일: 첫 번째 5000일 (Everydays: The First 5,000 Day)
    - https://ipfs.io/ipfs/QmXkxpwAHCtDXbbZHUwqtFucG1RMS6T87vi1CdvadfL7qA



- ERC-721: 이더리움의 NFT 표준 인터페이스
  - https://eips.ethereum.org/EIPS/eip-721
  - 표준API와 자연어로 된 설명





#### ■ ERC-721 함수

- balanceOf: 파라미터로 전달받은 주소가 보유하고 있는 NFT 수량 반환
- ownerOf : 파라미터로 전달 받은 NFT를 소유하고 있는 주소 반환
- safeTransferFrom : 전송받을 주소(\_to)가 NFT 토큰을 받을 수 있는지 검증하고 전송 진행
- transferFrom : NFT 소유 주소로부터 다른 주소로 토큰 전송
- approve : 파라미터로 전달 받은 주소에 NFT 전송 권한 부여
- setApprovalForAll : 파라미터로 전달 받은 주소에 소유자(msg.sender)의 모든 NFT 전송 권한 부여 또는 해제
- getApproved : 파라미터로 전달 받은 NFT 토큰에 대한 권한이 있는 주소 반환
- isApprovedForAll : setApprovalForAll 의 실행 권한 여부 반환



#### ■ ERC-721 이벤트

- event Transfer(address indexed \_from, address indexed \_to, uint256 indexed \_tokenId)
  - NFT의 소유권이 변경될 때
  - NFT가 생성되고(`from` == 0) 소멸될 때(`to` == 0) 발생
- event Approval(address indexed \_owner, address indexed \_approved, uint256 indexed \_tokenId)
  - 한 NFT의 승인(approved) 주소가 변경되거나 재확인 때 발생, 0 주소는 승인된 주소가 없음을 나타냄
- event ApprovalForAll(address indexed \_owner, address indexed \_operator, bool \_approved)
  - 소유자에 대해 운영자가 활성화되거나 비활성화될 때 발생, 운영자는 소유자의 모든 NFT를 관리할 수 있음



#### ■ ERC-165 인터페이스

- 스마트 컨트랙트가 어떤 인터페이스를 지원하는지 식별하는 표준: "Standard Interface Detection" 규약
- 다른 스마트 컨트랙트나 외부 애플리케이션은 ERC-165를 통해 어떤 기능이 지원되는지 알 수 있음
- 컨트랙트가 `interfaceId`로 정의된 인터페이스를 구현했으면, 참(true)을 반환
  - ERC165♀ interfaceId: type(ERC165).interfaceId
    - bytes4(keccak256('supportsInterface(bytes4)')) = 0x01ffc9a7
  - ERC721♀ interfaceId: type(ERC721).interfaceId
    - 모든 함수의 selector를 비트 단위 xor 연산(0x80ac58cd)

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



#### ERC-721 Receiver

- ERC-721 토큰 수신자 인터페이스
- ERC-721 토큰 컨트랙트에서 safeTransfer가 이루어질 때 받는 계정이 토큰을 전송 받을 수 있는 계정인지 아닌지에 대한 검증 표준을 제공
  - 받는 계정(컨트랙트 계정)에 ERC721TokenReceiver interface가 존재하는지 즉 onERC721Received가 구현 되어 있는지 확인
  - 반환: bytes4(keccak256("onERC721Received(address,address,uint256,bytes)"))

```
interface ERC721TokenReceiver {
  function onERC721Received(address _operator, address _from, uint256 _tokenId, bytes memory _data)
external returns(bytes4);
}
```



#### ■ ERC-721 NFT 스마트 컨트랙트 개발 실습: ERC721StdNFT

```
interface ERC165 {
  function supportsInterface(bytes4 interfaceID) external view returns (bool);
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 calldata 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 ERC721TokenReceiver {
  function on ERC721Received (address operator, address from, uint 256 tokenId, bytes calldata data) external returns (bytes 4);
```



#### ■ 생성자와 데이터

```
contract ERC721StdNFT is ERC721 {
 address public founder;
 // Mapping from token ID to owner address(각 NFT의 소유자 주소)
 mapping(uint => address) internal ownerOf;
 // Mapping owner address to token count(특정 주소가 보유한 NFT의 개수)
 mapping(address => uint) internal balanceOf;
 // Mapping from token ID to approved address(특정 NFT를 대신 전송할 권리를 부여받은 주소를 저장)
 mapping(uint => address) internal approvals;
 // Mapping from owner to operator approvals(특정 주소가 소유자의 모든 NFT를 관리할 권한이 있는지)
 mapping(address => mapping(address => bool)) public operatorApprovals;
 string public name;
 string public symbol;
 constructor (string memory name, string memory symbol) {
   founder = msg.sender;
   name = name;
   symbol = symbol;
   for (uint tokenID=1; tokenID<=5; tokenID++) {</pre>
     mint(msg.sender, tokenID);
```



- 내부함수 \_mint()
  - 새 토큰을 발행하기 위한 내부 함수

```
function _mint(address to, uint id) internal {
    require(to != address(0), "mint to zero address");
    require(_ownerOf[id] == address(0), "already minted");

    _balanceOf[to]++;
    _ownerOf[id] = to;

emit Transfer(address(0), to, id);
}
```

■ mintNFT(): 새 토큰 발행

```
function mintNFT(address to, uint256 tokenID) public {
   require(msg.sender == founder, "not an authorized minter");
   _mint(to, tokenID);
}
```



#### ■ 상태변수 값 확인

```
function ownerOf(uint256 _tokenId) external view returns (address) {
  address owner = ownerOf[ tokenId];
  require(owner != address(0), "token doesn't exist");
  return owner;
function balanceOf(address owner) external view returns (uint256) {
  require( owner != address(0), "balance query for the zero address");
  return _balanceOf[_owner];
function getApproved(uint256 tokenId) external view returns (address) {
  require( ownerOf[ tokenId] != address(0), "token doesn't exist");
  return approvals[ tokenId];
function isApprovedForAll(address owner, address operator) external view returns (bool) {
  return operatorApprovals[ owner][ operator];
```



- approve()
  - 주어진 토큰 ID의 전송을 다른 주소에게 허가
  - 토큰 소유자나 승인된 운영자만이 호출할 수 있음

```
function approve(address _approved, uint256 _tokenId) external payable {
   address owner = _ownerOf[_tokenId];
   require(
     msg.sender == owner || _operatorApprovals[owner][msg.sender],
     "not authorized"
   );
   emit Approval(owner, _approved, _tokenId);
}
```



- setApprovalForAll()
  - 주어진 운영자의 승인을 설정 또는 해제
  - 운영자가 발신자를 대신해 모든 토큰을 전송할 수 있도록 허가 또는 해제



- transferFrom()
  - 주어진 토큰 ID의 소유권을 다른 주소로 전송
  - msg.sender는 소유자, 승인된 주소, 운영자여야 함

```
function transferFrom(address from, address to, uint256 tokenId) external payable {
  _transferFrom( _from, _to, _tokenId);
function _transferFrom(address _from, address _to, uint256 _tokenId) private {
  address owner = ownerOf[ tokenId];
  require( from == owner, "from != owner");
  require( to != address(0), "transfer to zero address");
  require(msg.sender == owner
      || msg.sender == approvals[ tokenId]
      | operatorApprovals[owner][msg.sender]); //"msg.sender not in {owner,operator,approved}");
  emit Transfer( from, to, tokenId);
```



- safeTransferFrom()
  - 주어진 토큰 ID의 소유권을 다른 주소로 안전하게 전송
  - 만일 목표 주소가 컨트랙트라면, 해당 컨트랙트는 `onERC721Received`를 구현했어 야만 함
    - ERC721TokenReceiver.onERC721Received.selector:
       bytes4(keccak256("onERC721Received(address,address,uint256,bytes)"))

```
function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes calldata data) external payable {
    _transferFrom(_from, _to, _tokenId);

    require(
    _to.code.length == 0 ||
        ERC721TokenReceiver(_to).onERC721Received(msg.sender, _from, _tokenId, data) ==
        ERC721TokenReceiver.onERC721Received.selector,
        "unsafe recipient"
    );
}
```

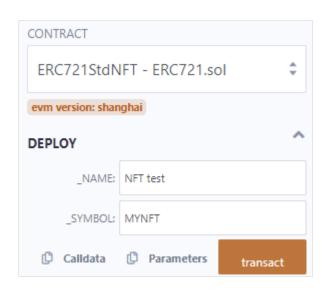


■ ERC-165 구현

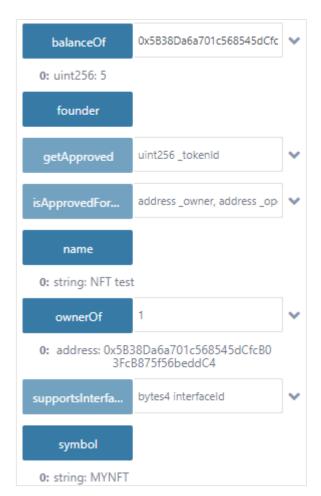
```
function supportsInterface(bytes4 interfaceId) external pure returns (bool) {
   return
   interfaceId == type(ERC721).interfaceId ||
   interfaceId == type(ERC165).interfaceId;
}
```



- 테스트
  - 배포: 이름,심볼
    - 5개의 NFT 토큰을 배포자가 가지고 있음

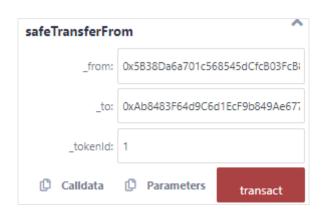








- 테스트
  - 전송



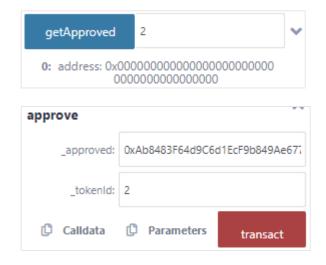


```
"event": "Transfer",
"args": {
        "0": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
        "1": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
        "_from": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
        "_to": "0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2",
        "_tokenId": "1"
                   0x5B38Da6a701c568545dCfc >
    balanceOf
   0: uint256: 4
    balanceOf
                   0xAb8483F64d9C6d1EcF9b84 >>
  0: uint256: 1
     ownerOf
  0: address: 0xAb8483F64d9C6d1EcF9b849A
              e677dD3315835cb2
```



# ■ 테스트

Approve



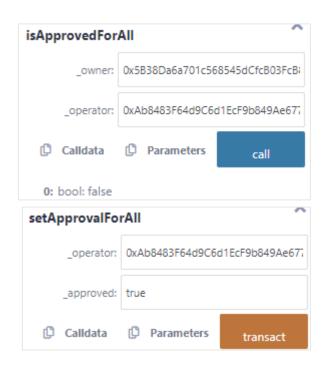


e677dD3315835cb2

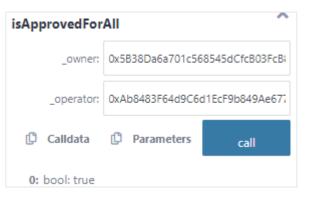


# ■ 테스트

setApprovalForAll

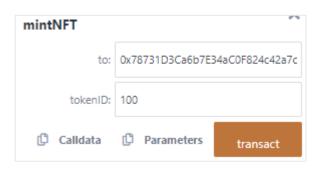








- 테스트
  - 새 NFT 발행

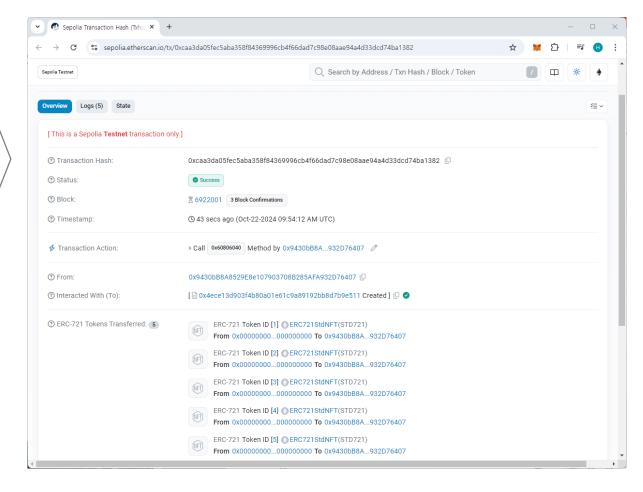






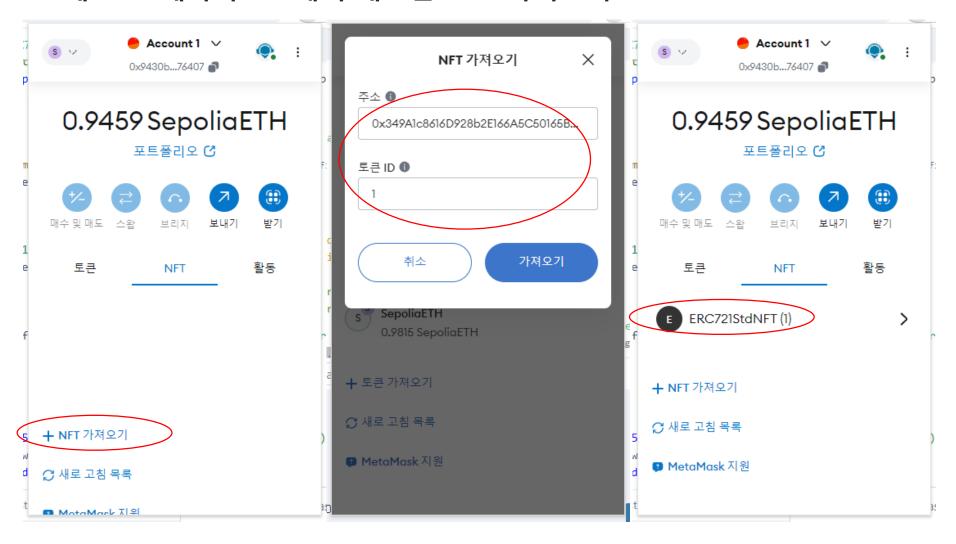
■ 테스트: remix에서 Sepolia 테스트 네트워크에 배포

ENVIRONMENT	₩ i	
Sepolia Testnet - MetaMask		Γ
Sepolia (11155111	1) network	
DEPLOY	^	
_NAME:	ERC721StdNFT	
_SYMBOL:	STD721	
( Calldata	Parameters transact	



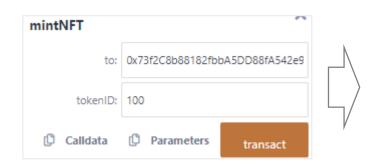


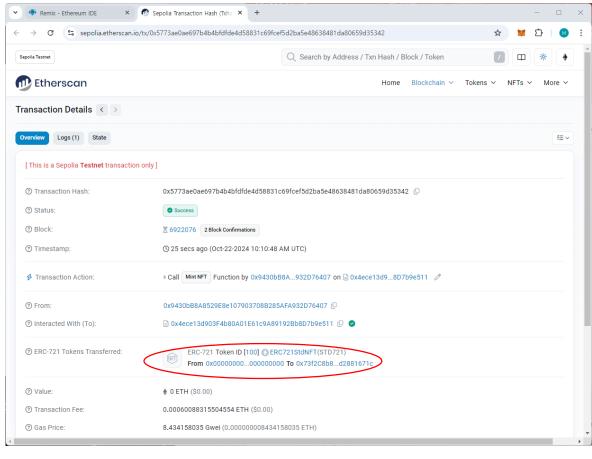
■ 테스트: 메타마스크에서 배포한 NFT 가져오기





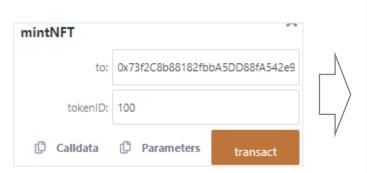
- 테스트: 새 NFT Sepolia 테스트 네트워크 배포
  - 새 NFT 발행

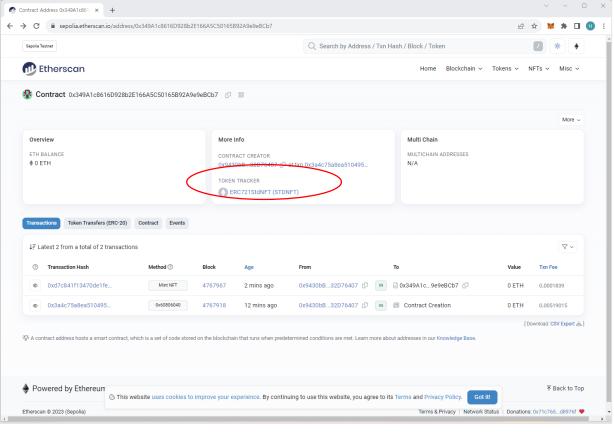






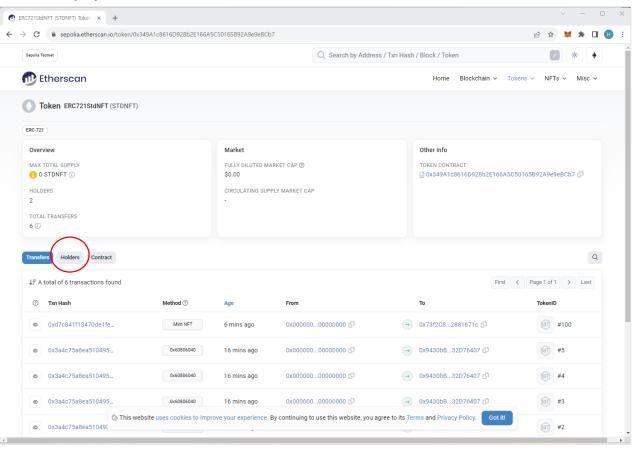
- 테스트(테스트 네트워크 배포)
  - 새 NFT 발행: 이더스캔 컨트랙트 정보 화면
    - https://sepolia.etherscan.io/address/0x4ece13d903f4b80a01e61c9a89192bb8d7b9e511







- 테스트(테스트 네트워크 배포)
  - 이더스캔 [More Info] -> [TOKENTRACKER]
    - 토큰 전송 기록





- 테스트(테스트 네트워크 배포)
  - 이더스캔 [More Info] -> [TOKENTRACKER] -> [Holders]
    - 소유자 정보 페이지

