명진가Z

현명한 명품 소비를 위한 이더리움 기반 럭셔리 거래 플랫폼

강동석 공윤환 임형준 정언용



01. 프로젝트 기획 배경

02. 기술소개

03. 주요 기능

04. 기대효과

05. 시연

06. Q&A

프로젝트 기획 배경









명품을 좋아하는 28세, 김싸피

"온라인으로 명품을 찾아보고 있어요."

"마음에 든다면 중고 상품이라도 구매하고 싶어요"

"그런데 제가 산 명품이 **진품**이 확실할까요**?**"

프로젝트 기획 배경

무신사·네이버 '크림', 짝퉁 명품 놓고 충돌

'수수료 제로 종료' 리셀업계 1위 크림, 수수료 부과·배송료 인상 나선다

크림, 내달 21일부터 구매자 수수료 1% 부과·5월부터 배송비 인상 업계 2위 솔드아웃 "당분간 수수료 인상 계획 없지만, 정책 변동 가능성 있다"

기술소개 - 흐름

smartContract - react 연결 흐름



기술소개 - solidity 코드 작성

smartContract 코드 작성 - using solidity

```
contract MintProduct is ERC721Enumerable {
   constructor() ERC721("h662Animals", "HAS") {}

mapping(uint256 => ProductData) public products;
```

contract = java의 class와 비슷한 개념

```
function mintProduct(
    string memory brand,
    string memory name,
    string memory productType,
    string memory serialNum
) public {
    uint256 productId = totalSupply() + 1;
    ProductData memory p;
    p.productId = productId;
    p.brand = brand;
    p.name = name;
    p.productType = productType;
    p.serialNum = serialNum;
    products[productId] = p;
    _mint(msg.sender, productId);
```

기술소개 - solidity 코드 작성

smartContract 코드 작성 - using solidity

MintProduct의 mintProduct()를 이용해서
 minting

민팅(Minting) 이란 그림이나 영상 등 디지털 자산의 대체불가능토큰 (NFT)을 생성하는 것을 일컫는 용어다

출처: 연합인포맥스(http://news.einfomax.co.kr)

```
function mintProduct(
    string memory brand,
    string memory name,
    string memory productType,
    string memory serialNum
) public {
    uint256 productId = totalSupply() + 1;
    ProductData memory p;
    p.productId = productId;
    p.brand = brand;
    p.name = name;
    p.productType = productType;
    p.serialNum = serialNum;
    products[productId] = p;
    _mint(msg.sender, productId);
```

기술소개 - solidity 코드 작성

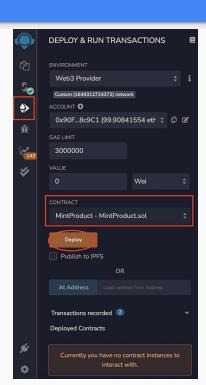
smartContract 코드 작성 - using solidity

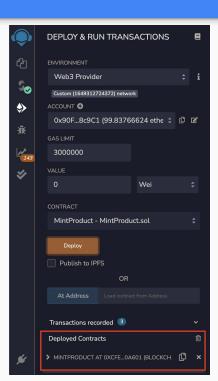
NFT가 배포된 컨트렉트의 주소를
 SaleProduct 넘겨준다

```
contract SaleProduct {
   MintProduct public mintProductContract;

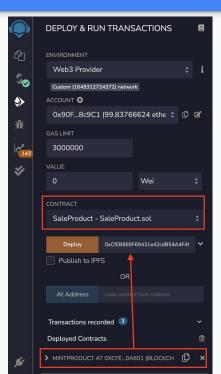
constructor(address _mintProductAddress) {
   mintProductContract = MintProduct(_mintProductAddress);
}
```

• MintProduct 배포



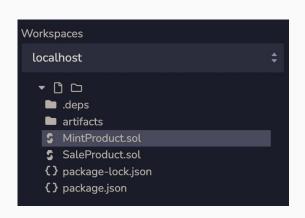


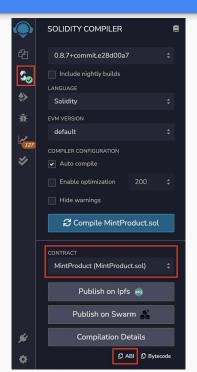
• SaleProduct 배포

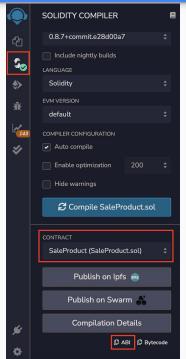




remix ide를 이용한 배포 - using solidity







• ABI 생성

cf) ABI(Application Binary Interface) 란?

API와 비슷한 개념. 다른 소프트웨어간 인터페이스를 정의하는 것

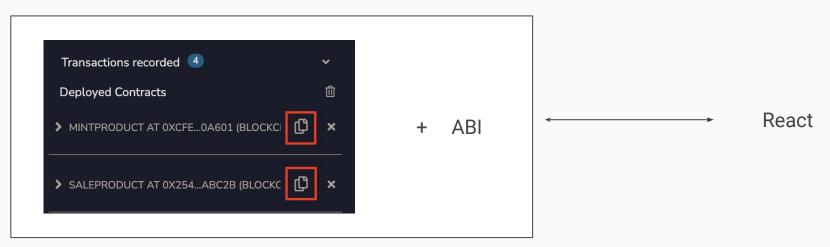
- 차이점
 - o API는 소스 코드 level에서 인터페이스를 정의
 - ABI는 특정 아키텍쳐 level에서 동작하는 소프트웨어 사이의 바이너리 인터페이스를 정의

참조 링크

- https://medium.com/pocs/ethereum-abi%EC%99%80-%EA%B4%80%EB %A0%A8%EB%90%9C-q-a-%EC%A0%95%EB%A6%AC-40e639ee1a03
- https://hucet.tistory.com/46

기술소개 - react와 smart contract 연결

smartContract 코드 작성 - using solidity



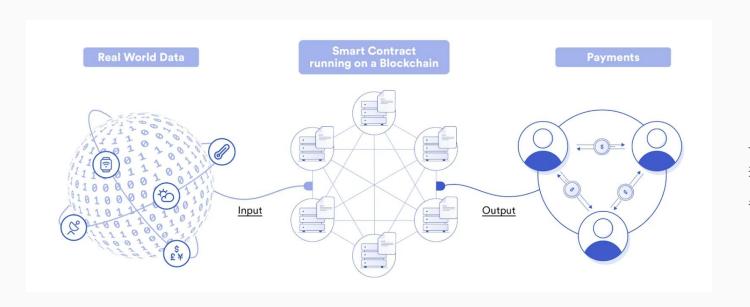
기술소개 - react와 smart contract 연결

```
export const mintProductContract = new web3.eth.Contract(
mintProductAbi,
mintProductAddress
);

export const saleProductContract = new web3.eth.Contract(
saleProductAbi,
saleProductAddress
);
```

연결 성공!

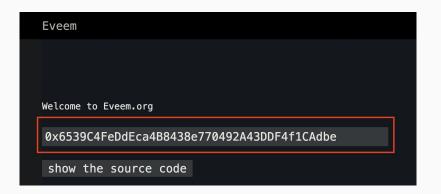
기술소개 - react와 smart contract 연결



누구나 스마트 컨트렉트의 코드를 볼 수 있다!

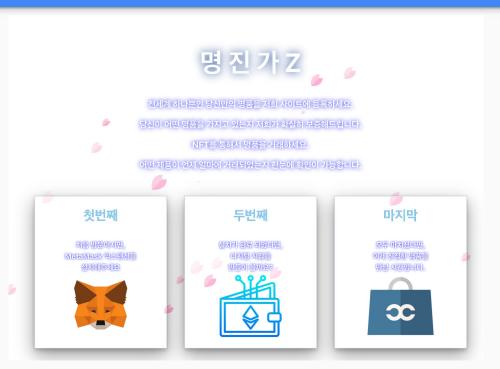
기술소개 - 디컴파일

https://eveem.org/



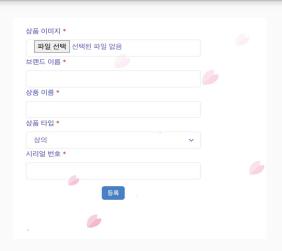
배포된 컨트렉트의 주소

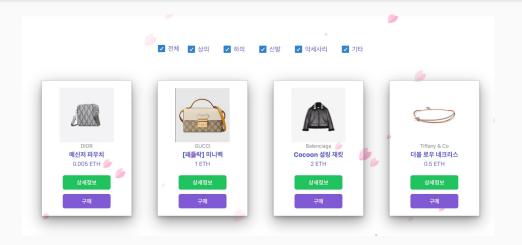
```
0x6539C4FeDdEca4B8438e770492A43DDF4f1CAdbe
                                                                                see random
         # Panoramix 17 Feb 2020
</>>
Code
         def storage:
Φ°
           unknown7d635a5eAddress is addr at storage 0
           unknowne7bf7dfc is mapping of uint256 at storage 1
Json
           unknowne3811eaa is array of struct at storage 2
           unknowne16305d9 is array of uint256 at storage 3
₩
Asm
         def unknown369e2f3c(): # not payable
           return unknowne16305d9.length
         def unknown38eb6a19(uint256 _param1): # not payable
Abi
           require calldata.size - 4 >= '32
           require param1 == param1
 return unknowne7bf7dfc[_param1]
Data
         def unknown7d635a5e(): # not payable
           return unknown7d635a5eAddress
         def unknowne16305d9(uint256 _param1): # not payable
           require calldata.size - 4 >= ' 32
           require param1 == param1
           require param1 < unknowne16305d9.length
           return unknowne16305d9[_param1]
         def unknowne3811eaa(uint256 _param1, uint256 _param2): # not payable
           require calldata.size - 4 >= '64
           require _param1 == _param1
           require param2 == param2
           require param2 < unknowne3811eaa[ param1].field 0</pre>
           return unknowne3811eaa[_param1][_param2].field_0, unknowne3811eaa[_param1][_param2].field_256
```



메인 페이지

- 페이지 소개
- 메타마스크 설치 방법
- 블록체인 지갑 등록
- 제품 등록 및 NFT발행

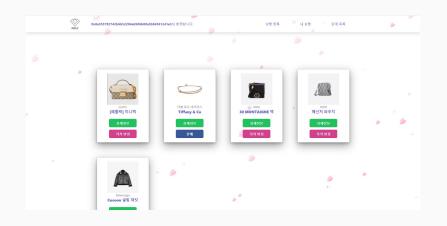




일반 회원: 상품 거래 가능

기업 회원: 상품 등록 + 거래 가능

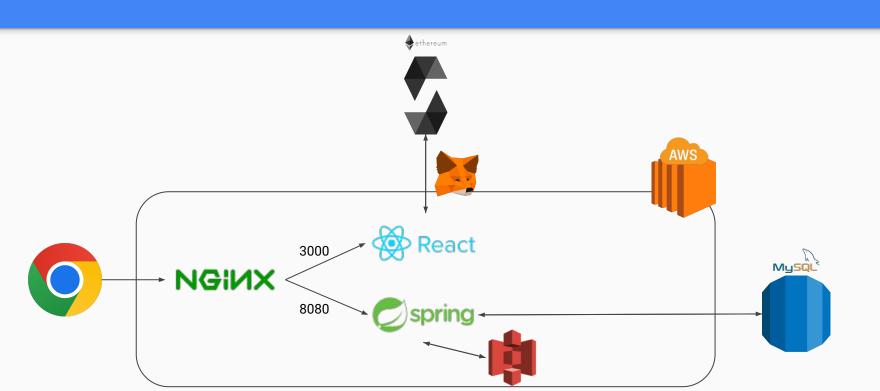
현재 거래 가능한 상품 목록

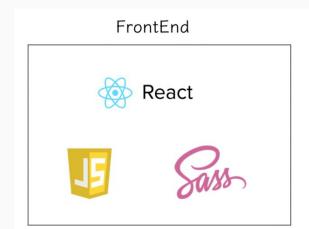


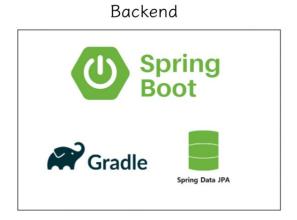


현재 자신이 보유중이거나 판매중인 상품

해당 상품에 대한 상세정보 및 거래 내역









기대효과

거래시 매번 부담스러웠던 수수료를 낮추고, 상품 등록시마다 NFT를 발행함으로써 위변조가 불가능한 특성을 이용하여 해당물품의 진품임을 보증하고, 안심거래를 제공합니다. 시연

Q&A

발표 내용에 관해

궁금한 점이 있으시다면

자유롭게 질문해주세요!

감사합니다.