

ERC-20

☰ 태그

ERC

ERC-20

- 태그: 작성하려는 글에 맞거나 연관되어 있는 태그를 선택합니다.
- 상태: 해당 글의 상태를 의미합니다.
 - 글을 쓸 예정으로 등록했다면 **작성 예정**, 글을 쓰는 중이거나 아직 완료한 것 같지 않다면 **작성 중**, 완료 후에는 **완료**로 표기합니다.

▲가독성을 위해 개요와 결론을 작성하시는 것을 추천하지만, 느낌에 따라 자유롭게 작성하시면 됩니다!

개요

ERC-20의 필요성

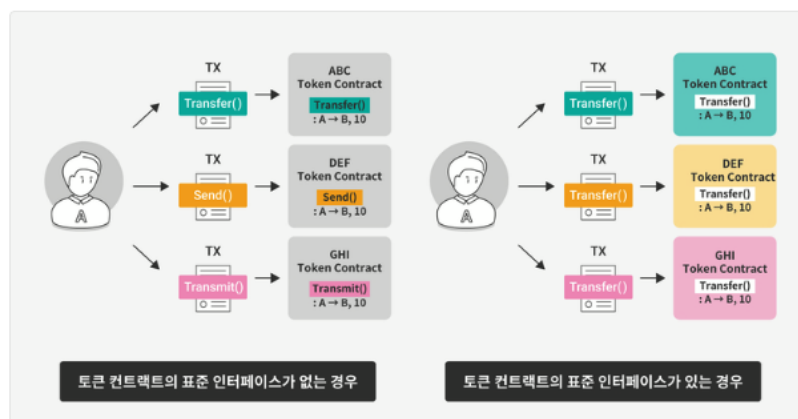
이더리움의 코인인 이더의 경우, 여러분의 지갑에 생성된 개인키의 계정이고, 블록체인 상의 계정에서 코인을 보관하고 있다.

하지만 ERC-20 토큰의 경우에는 토큰을 발행한 컨트랙트가 존재하고, 컨트랙트에 여러분의 계정이 얼마를 가지고 있는지를 나타내주는 방식으로 표현된다.

예를 들어, ABC 토큰 컨트랙트에서 Alice가 Bob에게 10 ABC를 전송한다고 가정해보자.

Alice는 개인키로 서명된 트랜잭션을 블록체인에 제출할 것이고, 토큰 컨트랙트에서는 Alice가 10 ABC를 가지고 있을 경우, Bob에게 10 ABC 토큰을 이전하는 동작을 실행한다.

이렇게 작동하는 기능의 이름을 컨트랙트 상에서 transfer라고 표기해두었다고 해보자. 그런데 ABC 토큰만 있는 게 아니라, DEF 토큰, GHI 토큰도 있을 텐데, 각 컨트랙트에는 send, transmit 이라고 해둔다면, 서로 교환도 어려울 뿐더러, 지갑에서 구현이 어려워 질 수가 있다. 그래서 ERC-20은 이러한 상황을 방지하기 위해 표준 인터페이스로 제안된 것이다.



본론

ERC-20의 내용

ERC-20에는 다음과 같은 함수가 정의되어 있다.

```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)

function totalSupply() public view returns (uint256)

function balanceOf(address _owner)
public view returns (uint256 balance)

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

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

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

function allowance(address _owner, address _spender)
public view returns (uint256 remaining)
```

스테이블 코인으로 유명한 USDT를 가지고 ERC-20 토큰의 함수의 사용을 간단하게 예시를 들어 살펴보자.

USDT 토큰의 이름은 'Tether USD' 이고, 심볼은 'USD' 로 표기된다.

만약 블록체인 상에서 토큰을 발행할 때 이름과 심볼을 정의하고 싶다면, ERC-20의 name()과 symbol() 함수에 정의하면 된다. 또한, 토큰을 발행하는 수량과 유통량을 고려했을 때 화폐의 단위를 어느정도로 할 지를 나타내기 위해서 decimals 을 사용한다.

이외에도 각 함수는 다음과 같은 경우에 사용된다. 토큰 컨트랙트는 하나의 장부라고 생각하시고, 장부에 기입된 내용을 어떻게 요청하여 알아낼 수 있을까를 생각하며 다음 함수의 이름을 생각해보면 이해가 쉬울것이다.

- totalSupply 는 토큰의 발행 총량을 알 수 있는 인터페이스이다.
- balanceOf 는 요청한 계정의 잔액이 얼마인지를 알기 위해 사용된다.
- transfer 는 토큰을 다른사람에게 이전하기 위해 사용된다.
- approve 는 다른 사람에게 정해진 금액 만큼 인출할 권리를 부여한다.
- allowance 는 다른 사람에게 허가한 금액의 허용 잔액이 얼마인지를 나타낸다.
- transferFrom 은 승인된 허가를 받은 사람이 토큰을 보낼 때 사용된다. 예를 들어, 여러분의 잔액을 A가 허가하여 B에게 전송하는 경우이다. 사전에 approve를 통해 승인이 되어 있어야 한다.

또한 이외에도 위에서 설명한 함수가 실행되면 알려주는 기능인 Events가 두가지 있다.

이벤트가 상대적으로 적은 이유는 자산이 이동되거나, 이동 가능성을 나타내는 경우가 두 가지 경우 뿐이기 때문이다. 이름이 무엇인지, 누군가가 조회해 보았는지와 같은 상황은 자산의 변동에 해당되지 않기 때문에 특별히 이벤트

가 발생하지 않는다. 예를 들어, `transfer`(함수)가 실행되어, 자산의 이동이 일어나면, 이 내역에 대한 `Transfer`(이벤트)가 발생한다.

```
event Transfer(address indexed _from, address indexed _to, uint256 _value)
event Approval(address indexed _owner, address indexed _spender, uint256 _value)
```

이렇게 알고보니, 여러분의 지갑에서 표시되는 토큰의 이름, 심볼, 화폐 단위나 잔액 등이 ERC-20 토큰 컨트랙트로 부터 가져온 정보라는 것을 알 수 있다. 그리고 다른 사람에게 토큰을 전송할 경우에는 토큰 컨트랙트에 `transfer`, `approve`, `allowance`와 같은 기능을 사용한다는 것도 알 수 있다. 이를 모든 토큰마다 동일하게 적용한 ERC-20이 있으면 개발할 때도 쉽게 추가가 가능하기 때문에 매우 편리하다.

ERC-20은 이더리움에 해당하는 표준 인터페이스를 나타내지만, 각 블록체인 네트워크 마다 토큰을 발행할 때 사용하는 표준이 존재한다.

ERC-20의 장단점

ERC-20의 장점

1. 대체 가능성

ERC-20 토큰은 다른 토큰을 대체할 수 있다. 대체 가능하다는 의미는 동등한 가치를 가지고 있으며, 더 작은 단위로 쪼개질 수 있다는 것을 뜻한다. 또한 ERC-20은 상호호환성을 보유하고 있다. 즉, ERC-20 기반 토큰은 동일한 이더리움 지갑으로 전송이 가능하다. 그렇기 때문에 현재 많은 DApp에서 자체 생태계 토큰을 ERC-20 기반으로 발행하고 있으며, 이더리움 네트워크 상에서 상호호환할 수 있다.

2. 유연성

유연성이란 ERC-20 토큰의 가장 큰 장점 중 하나로, ERC-20 특정한 개발을 제한하지 않는다. 개발자들은 적합한 부가적인 기능을 구현할 수 있으며 다양한 변수 설정이 가능하다. 이러한 특징 덕분에 ERC-20은 예술 작품이나 부동산 소유권 증명 등에도 활용되고 있다.

3. 대중성

대표적인 이더리움 토큰의 표준인 ERC-20은 활용성, 상호운용성 측면에서 장점을 가지고 있다. 따라서 현재 발행된 디지털자산의 90% 가량이 ERC-20 토큰을 기반으로 하고 있다.

ERC-20의 단점

1. 확장성

최근 DeFi 서비스들의 성장은 이더리움 네트워크 내에서 많은 트랜잭션을 발생시키며 이더리움 네트워크에 과부하를 일으키고 있다. 또한 이더리움 가격이 오를수록 트랜잭션의 승인 비용이 상승하여 네트워크 이용자들에게 비용적 부담을 가중시키기도 한다. 이는 ERC-20 토큰 사용 시 영향을 받을 수 있는 문제이다. 이더리움 커뮤니티는 이러한 문제를 해결하기 위하여 이더리움 2.0으로 통합하고 다양한 방식으로 업그레이드하기 위하여 노력하고 있다.

2. 스캠


ERC-20은 누구나 편리하게 토큰을 생성할 수 있는 대중성을 지니고 있다. 이처럼 누구나 쉽게 토큰을 발행할 수 있다는 것이 단점이 되기도 한다. 실제로 별다른 기능이 부여되어 있지 않은 ERC-20 기반 토큰을 발행하는 데에는 몇 분이 채 걸리지 않는다. 따라서 ERC-20 토큰에 투자 시에는 주의 깊게 분석한 후 투자해야 할 필요가 있다.

결론

참고

ERC-20이 무엇인가요? | D'CENT Academy


블록체인을 가진 메인넷 중 스마트 컨트랙트를 지원하는 플랫폼에서는 토큰 발행이 가능합니다. 예를 들어 이더리움에서 토큰을 발행하는 프로그램(스마트 컨트랙트)을 작성하여 등록할 수 있습니다. 이더리움에서 스마트 컨트랙트는 누구나 작성하여 배포할 수 있기 때문에, 토큰 발행

 <https://academy.dcentwallet.com/v/ko/terminology/what-is-erc-20>

D'CENT Academy



ERC-20 토큰이란? 장단점, 채굴 가능 여부까지!

CONTENTS1. ERC 정의2. 스마트 컨트랙트 표준 ERC-203. ERC-20 규칙4. ERC-20 장점5. ERC-20 단점6. ERC-20 토큰도 채굴 가능할까?  ERC 정의 ERC는 Ethereum Request for Comment의 약자로 이더리움 블록체인 네트워크에서 발행되는 토큰의 표준을


 <https://brunch.co.kr/@gapcha/162>

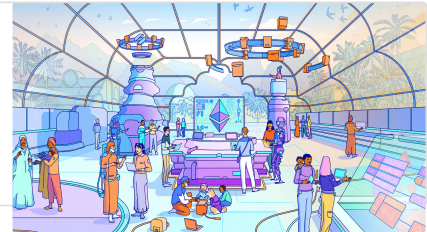
[블록체인정보]

ERC-20

ERC-20 Token Standard | ethereum.org

Ethereum is a global, decentralized platform for money and new kinds of applications. On Ethereum, you can write code that controls money, and build applications accessible anywhere in the world.

 <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/?ref=ansubin.com>



ERC20으로 토큰 배포 및 transfer

기본적으로 ERC20의 형식을 가지고 있는 인터페이스이다. 여기서 말하는 ERC20은 openzeppelin을 말한다.override는 말 그대로 부모 (IERC20)의 메서드를 오버라이드 했다는 뜻이다. balance는 사용자의 계좌잔액을 말하며, 여기서는 토큰의

 <https://velog.io/@ecoco97/ERC20으로-토큰-배포-및-transfer>

