

한 번에 끝내는 블록체인 개발 A to Z

Chapter 2

Blockchain 2.0 - Ethereum

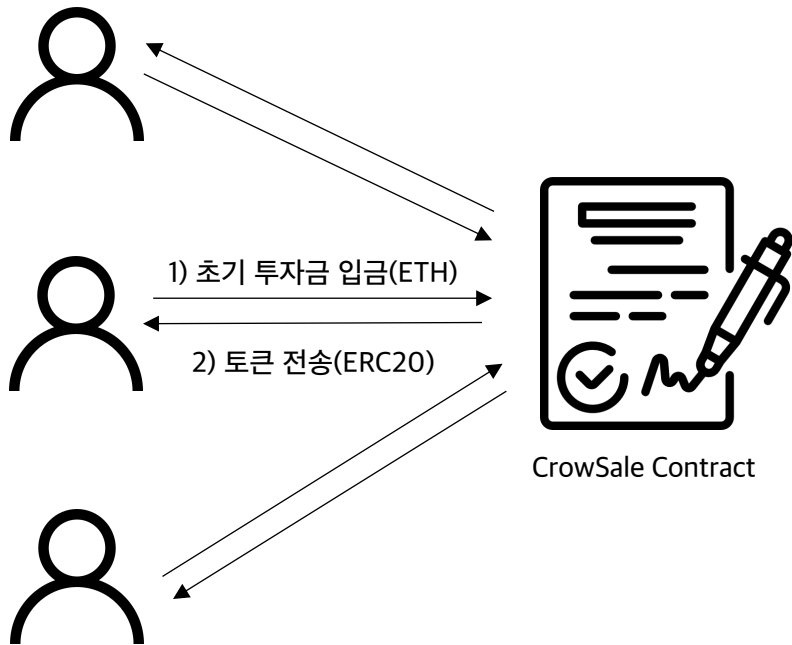
Chapter 2

Blockchain 2.0 - Ethereum

ERC-20

Initial Coin Offering

- Initial Coin Offering(ICO)란 블록체인 플랫폼 개발 자금 확보를 위해서 투자자들이 개발 자금을 투입하면 해당하는 금액만큼 Token을 발행해주는 것을 의미한다.
- Soft Cap, Hard Cap 등이 존재하여 특정 자금 이상이 모이지 않으면 자동 취소 되는 기능이 있다.
- 2017년 가상자산 시장이 활발하게 이루어진 이유는 ICO 붐 때문이다.



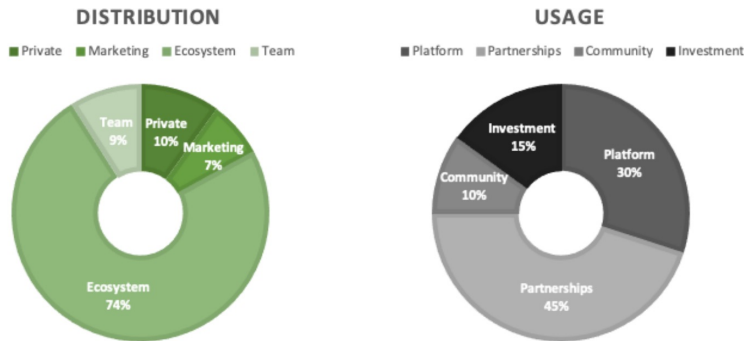
Token Distribution

- ICO의 가장 큰 장점은 서비스 오픈 전 사용자에게 투자금을 지급받고 개발자와 서비스 개발에 필요한 토큰을 미리 할당할 수 있는 점이다.
- 이러한 점은 추후에 ERC-20 Lock 기능과도 연관되어 일반적으로 개발사의 Token은 일정 기간 후에 매도가 가능하다.

ix) WEMIX Distribution Plan

A total of one billion WEMIX Tokens will be issued.

Among them, 10% will be distributed through private sales and utilized in initial stage of WEMIX growth. 7% will be utilized for marketing for platform vitalization. Another 9% will be allocated over a three-year period to members of WEMIX team who have contributed to or are likely to contribute to successful vitalization of WEMIX platform, and the remaining bulk of 74% will be used for supporting the long-term growth of the ecosystem.



(출처 : wemix whitepaper)

ICO의 대안

① IEO

중앙화된 거래소에서 초기 발행을 도와주는 방안입니다. 무분별한 발행 시장 대신 중앙화된 거래소가 선별하는 효과가 있고, 해당 거래소에 바로 거래가 되는 장점이 있습니다.

② IDO

탈중앙화된 거래소에서 지원하는 발행 방식입니다. 해당 DEX의 투표를 통하여 지원 여부를 결정하게 됩니다. 상장피등 중앙화된 거래소에서의 무분별한 상장 문제를 막을 수 있습니다.

ERC 20

장점

① 쉬운 발행 과정

메인넷 개발 없이 사용자에게 가치를 가질 수 있는 토큰을 Smart Contract 상으로 개발하여 배포할 수 있다.

② 발행량과 초기 관리

발행량이 제한 되어있는 ETH와 달리 초기 발행량을 조절하고, Blacklist 관리, 관리자 선임 등 다양한 기능을 코드상에서 구현이 가능하다.

③ Eth와 동일한 보안성

ETH와 마찬가지로 블록체인 상에서 관리되기에 안전성과 투명성 제공이 가능하다. 하지만 컨트랙트 상에 취약점이 있는 경우 매우 심각한 보안 취약성을 가지게 된다. 특정 주소의 잔액 정보는 CA의 storage에 저장된다.

ERC 20

표준

- EIP 20으로 제안된 새로운 토큰의 표준 스펙이다.
- 9가지의 Function과 2가지의 Event를 기본적으로 포함하여야 ERC20으로 보고 있지만, 구현 시에 함수의 수정이나 함수의 변경이 있더라도 주요 함수를 가지고 있다면 ERC 20으로 인식한다.

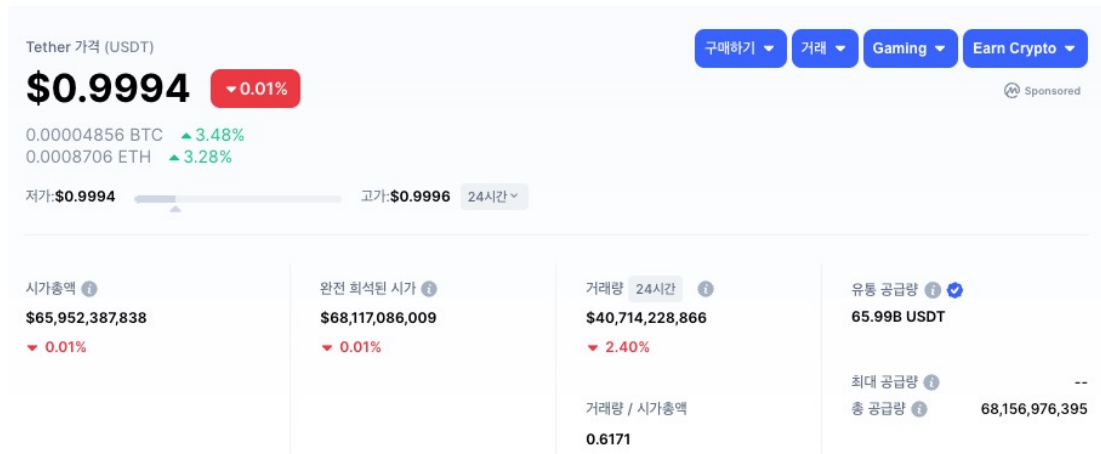
```
1  function name() public view returns (string)
2  function symbol() public view returns (string)
3  function decimals() public view returns (uint8)
4  function totalSupply() public view returns (uint256)
5  function balanceOf(address _owner) public view returns (uint256
   balance)
6  function transfer(address _to, uint256 _value) public returns (bool
   success)
7  function transferFrom(address _from, address _to, uint256 _value)
   public returns (bool success)
8  function approve(address _spender, uint256 _value) public returns
   (bool success)
9  function allowance(address _owner, address _spender) public view
   returns (uint256 remaining)

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

(출처 : ethereum.org)

발행량과 시가총액

- ERC20 뿐 아니라 모든 가상자산에서 투자자들이 중요하게 생각하는 것은 발행량과 시가총액이다.
- 발행량은 ERC20에서 totalSupply()에서 나오는 값이다. 총 발행량은 ERC20에 설정된 최대 발행량이다.
- 시가총액은 현재 발행량과 현재의 가격의 곱이 된다.



Stable Coin

① 법정화폐 담보

Tether, USDC 와 같이 1달러의 가치에 페깅되는 토큰이다. 예치된 달러 금액 만큼 발행 되기 때문에 항상 1 달러의 가치를 유지시킨다.

② 암호화폐 담보

MakerDAO의 DAI가 대표적이다. Defi의 서비스 중 하나로 Maker라는 담보 관리자가 일정 수수료를 지급받으며 담보의 가치를 조정하고 리스크 관리 업무를 진행합니다. MKR의 유동성 관리를 통하여 1달러의 가치를 유지시킵니다.

③ 알고리즘 기반

USDT와 같이 Terra-Luna 코인 페어의 유동성 차이를 이용한 알고리즘을 통해서 관리합니다. 지속적인 성장 가능성이 있어야만 가격이 유지될 수 있음을 Terra-Luna 사태로 증명되었습니다.

Wrapped ETH

① ERC20

ETH는 ERC20 표준을 지원하지 않기 때문에 ETH를 맡기고 동일한 수량의 wETH로 변환
wBTC, wTerra등 다양한 메인넷 코인들의 ERC20 버전이 존재한다.

② Defi 에서의 활용

Defi 플랫폼은 Smart Contract상에서 대부분의 ERC20 토큰들을 기반으로 설계 운영 중이기 때문에, 이에 맞는 ETH 또한 같은 기능의 지원이 필요하다.

③ Unwrap

ETH와 동일한 가치를 가지기 때문에, Unwrap을 Smart Contract에 요청을 하게되면 언제나 동일한 수량 만큼 ETH로 돌려받을 수 있다.