



# 블록체인DApp설계

## 2. 이더리움 기초

---

경기대학교 AI컴퓨터공학부 이재흥  
jhlee@kyonggi.ac.kr

# CONTENTS

## PRESENTATION



- 이더 화폐 단위
- 이더리움 지갑 선택하기
- 통제와 책임
- 메타마스크 설치하기
- 월드 컴퓨터 소개
- 외부 소유 계정 (EOA) 및 컨트랙트
- 간단한 컨트랙트: 테스트 이더 Faucet
- Faucet 컨트랙트 컴파일
- 블록체인에 컨트랙트 생성하기
- 컨트랙트 사용하기



## 이더 화폐 단위

- 이더(ether)
  - 이더리움의 화폐 단위
  - 이더리움은 블록체인 플랫폼을 의미하고, 이더가 화폐 단위를 의미

표 2-1 이더 명칭과 단위 명칭

값(웨이)	역지수	일반 이름	SI 이름
1	1	웨이(wei)	웨이
1,000	$10^3$	배비지(babbage)	킬로웨이(kilowei) 또는 펨토이더(femtoether)
1,000,000	$10^6$	러브레이스(lovelace)	메가웨이(megawei) 또는 피코이더(picoether)
1,000,000,000	$10^9$	샤넌(shannon)	기가웨이(gigawei) 또는 나노이더(nanoether)
1,000,000,000,000	$10^{12}$	사보(szabo)	마이크로이더(microether) 또는 마이크로(micro)
1,000,000,000,000,000	$10^{15}$	피니(finney)	밀리이더(milliether) 또는 밀리(milli)
1,000,000,000,000,000,000	$10^{18}$	이더(ether)	이더
1,000,000,000,000,000,000,000	$10^{21}$	그랜드(grand)	킬로이더(kiloether)
1,000,000,000,000,000,000,000,000	$10^{24}$		메가이더(megaether)



# 이더리움 지갑 선택하기

- 지갑(wallet)
  - 이더리움 계정을 관리하는 데 도움이 되는 소프트웨어 애플리케이션
  - 사용자의 키를 보유하고, 사용자를 대신하여 트랜잭션을 생성하고 브로드캐스트(broadcast) 할 수 있음

## 이더리움 지갑 추천

1. [베스트 월렛\(Best Wallet\)](#) – NFT, 탈중앙화 거래, 멀티체인을 지원하는 높은 보안 능력을 지닌 최고의 이더리움 지갑
2. [트레저\(Trezor\)](#) – 안전한 이더리움 하드웨어 지갑
3. [렛저\(Ledger\)](#) – 업계 최고의 하드웨어 이더리움 지갑
4. [오케이엑스\(OKX\)](#) – 2024년 최고의 보안과 기능을 자랑하는 코인 지갑
5. [크립토닷컴\(Crypto.com\)](#) – 안전하고 스테이킹을 지원하는 최고의 지갑
6. [바이낸스\(Binance\)](#) – 다양한 거래를 책임지는 최고의 지갑
7. [프라임XBT\(PrimeXBT\)](#) – 해킹 사례가 전혀 없는 안전한 지갑
8. [메타마스크\(MetaMask\)](#) – Web3 앱을 위한 최고의 암호화폐 지갑
9. [트러스트 월렛\(Trust Wallet\)](#) – NFT를 지원하는 사용자 친화적인 지갑



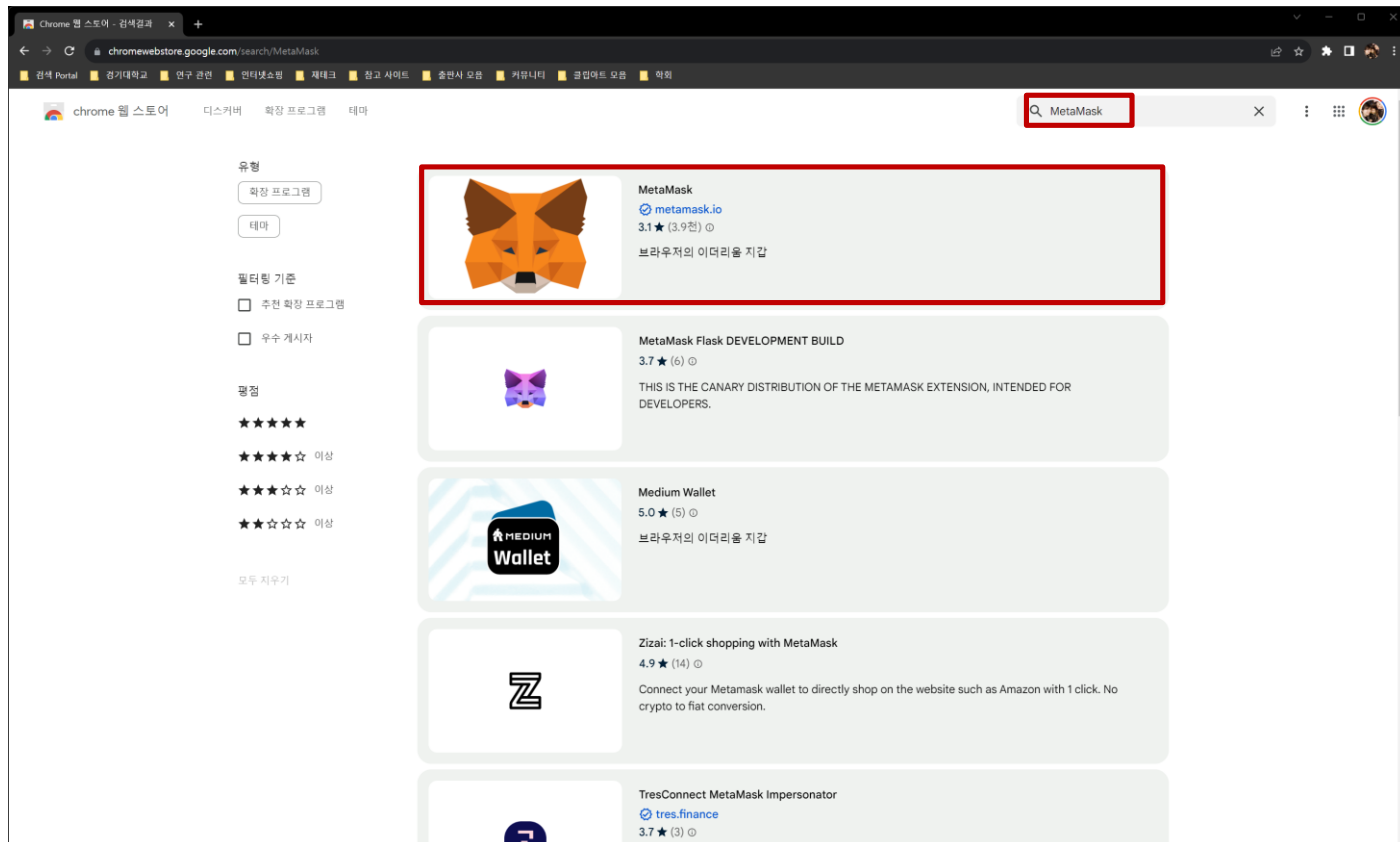
## 통제와 책임

- 핵심 관리 및 보안에 대한 기본 모범 사례
  - 개인키를 플레인 형태(plain form)로, 특히 디지털 형태로 저장하지 말 것
  - 개인키는 암호화된 형식으로 디지털 키저장소(keystore) 파일로 저장할 수 있음
    - 이 경우 키저장소 파일과 패스워드가 모두 있어야 계정에 접근할 수 있음
  - 많은 금액을 보내기 전에 먼저 소액을 보내서 트랜잭션이 잘 진행되는지 확인한 후 많은 금액을 보내는 방식을 사용

# 메타마스크 설치하기

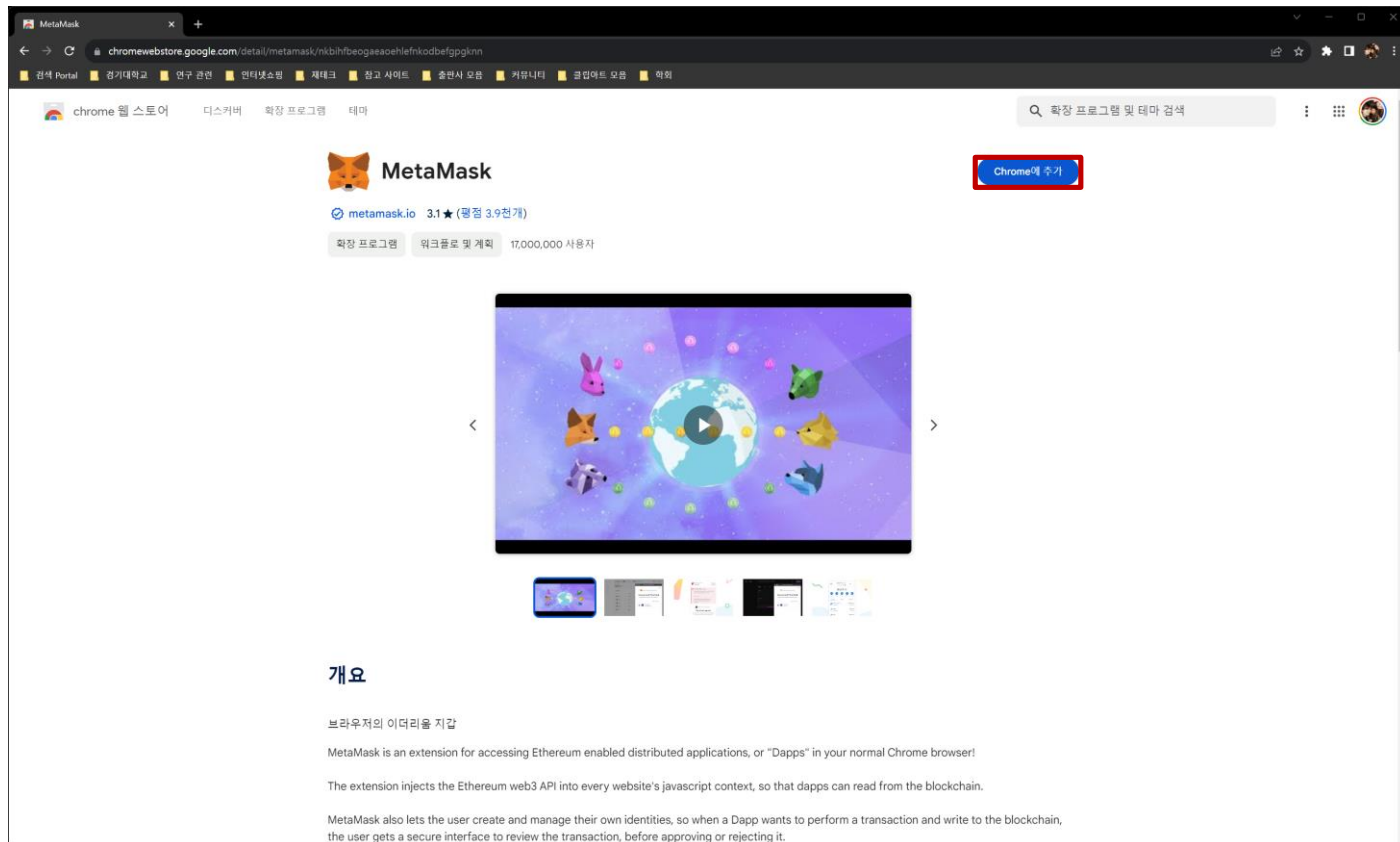
- 메타마스크 설치 과정

- <https://chromewebstore.google.com/> 접속
- MetaMask 검색



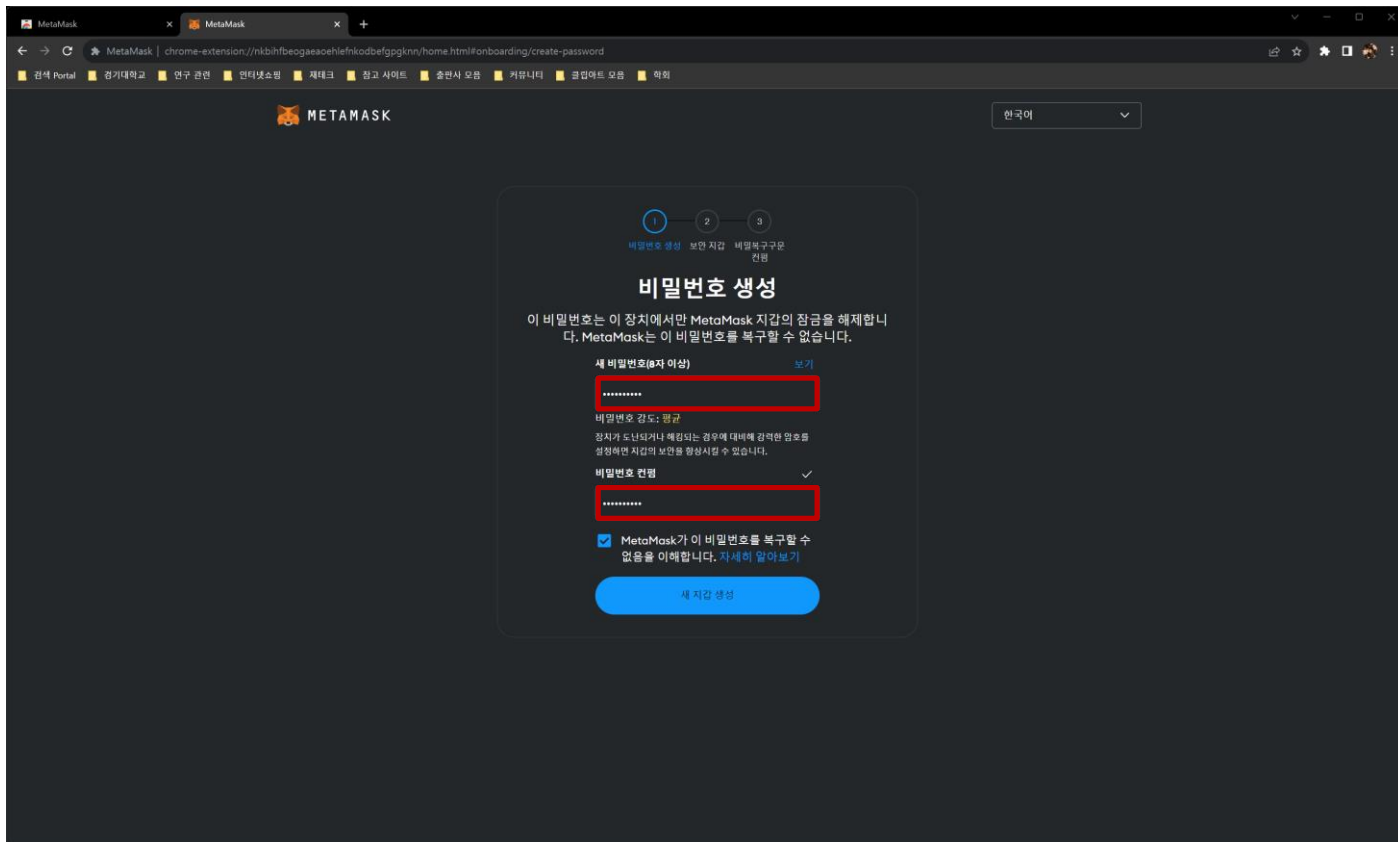
# 메타마스크 설치하기

- 메타마스크 설치 과정
  - ‘Chrome에 추가’ 클릭하여 설치



# 메타마스크 설치하기

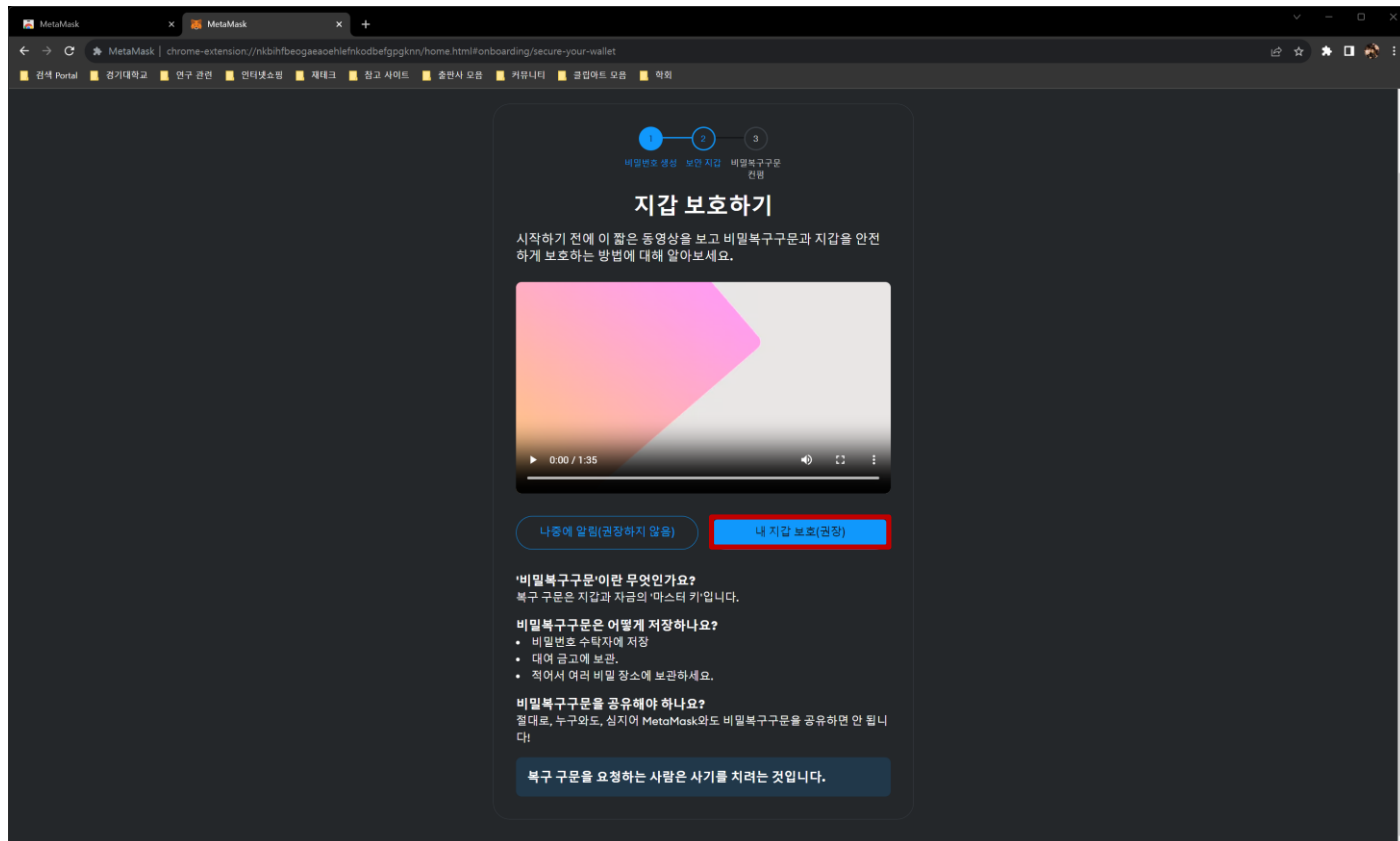
- 지갑 만들기
  - 이용약관 동의
  - 비밀번호 생성





# 메타마스크 설치하기

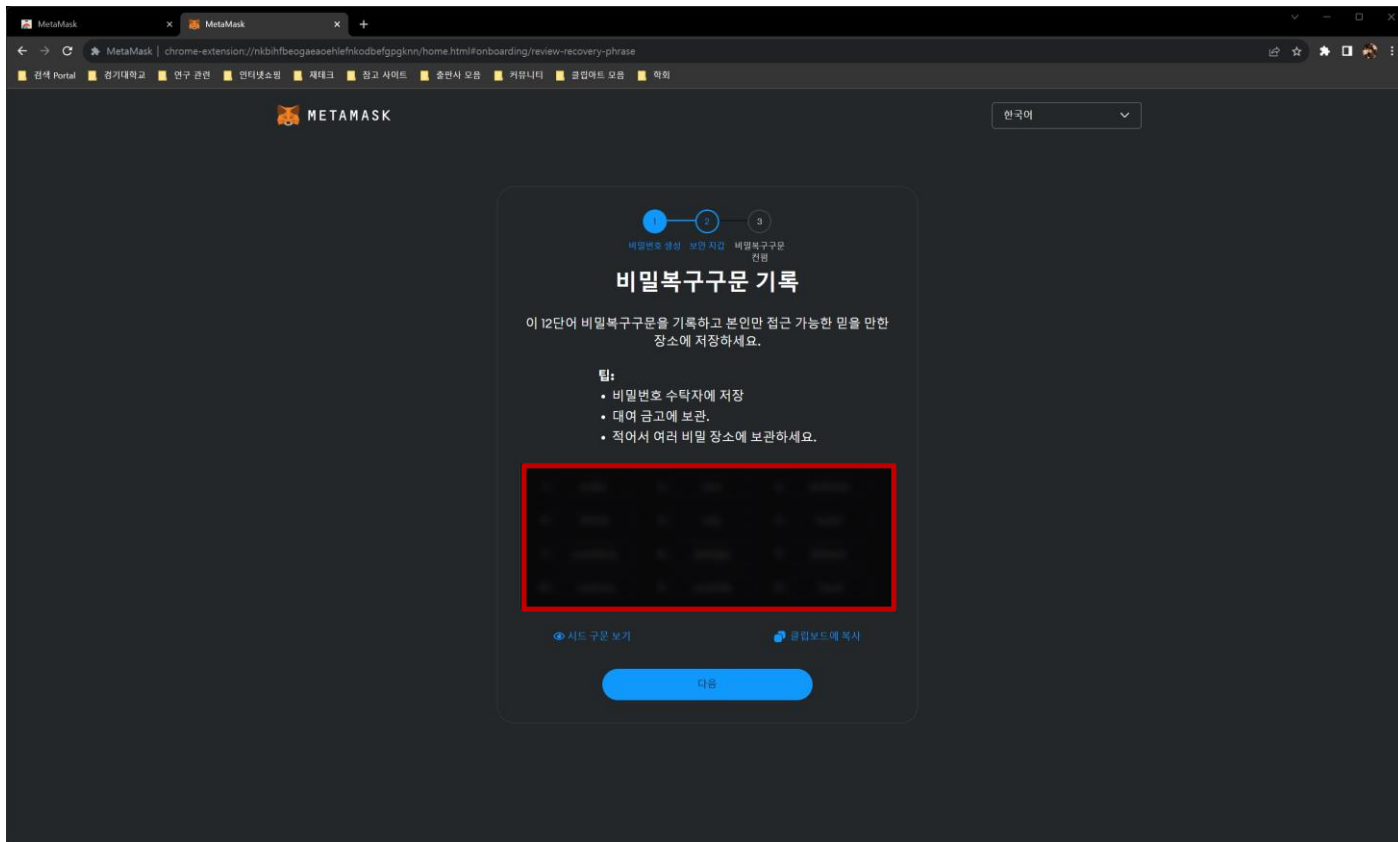
- 지갑 만들기
  - 지갑 보호하기
    - 내 지갑 보호(권장) 선택





# 메타마스크 설치하기

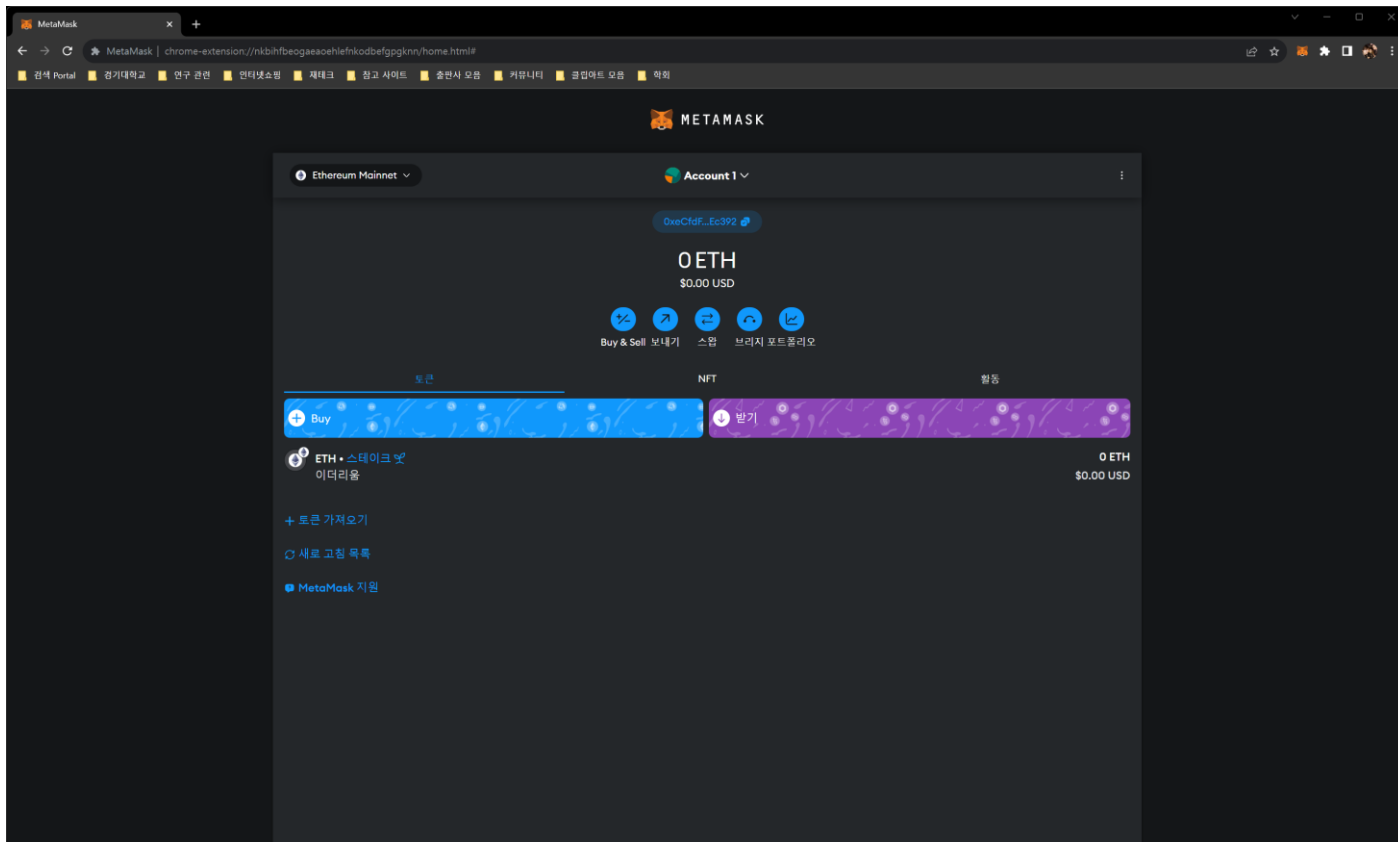
- 지갑 만들기
  - 비밀복구구문 기록 (12단어)
    - 실제 사용 지갑의 경우 절대 공개하지 말 것!!!





# 메타마스크 설치하기

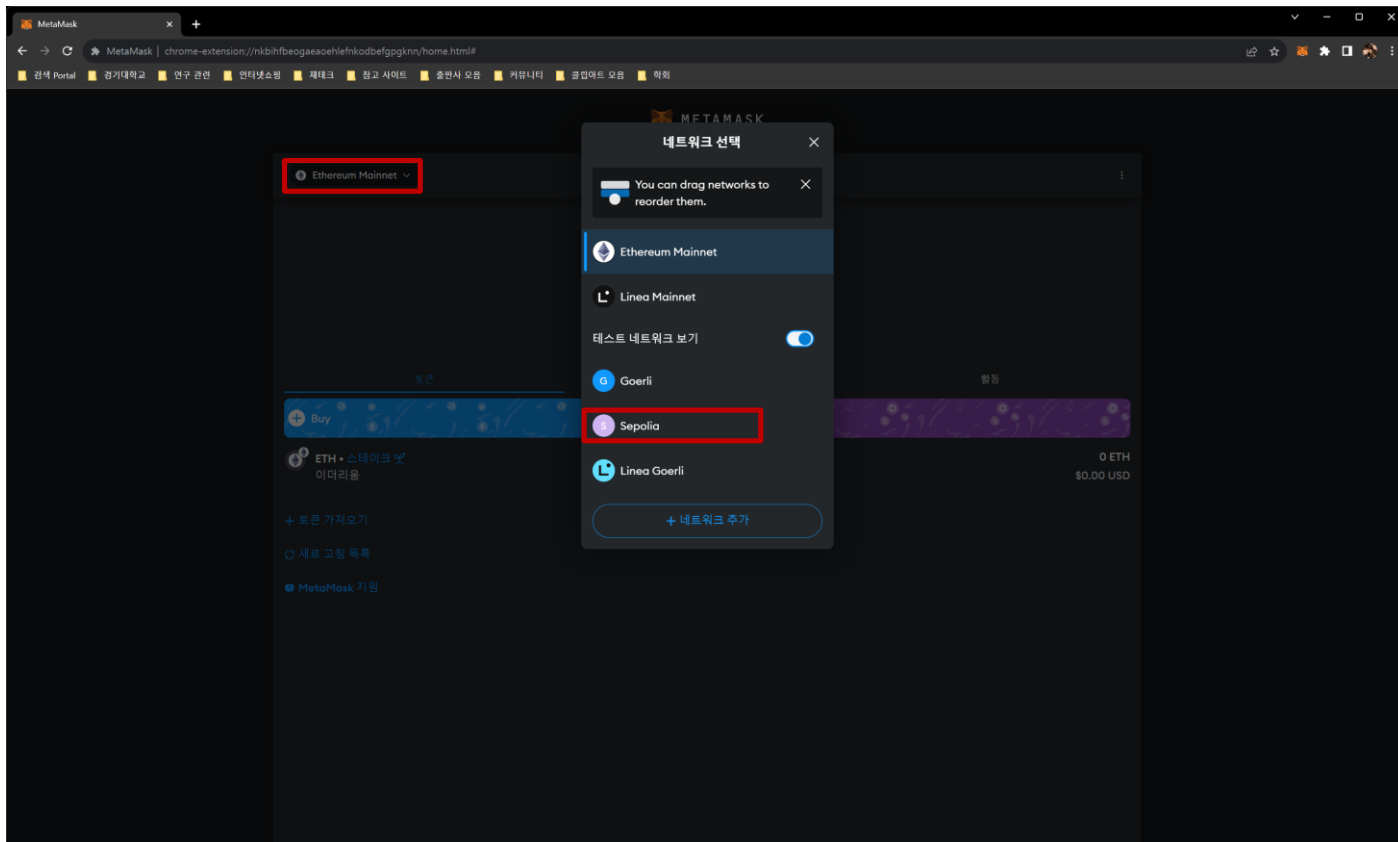
- 지갑 만들기
  - 비밀복구구문 컨펌
  - 지갑 생성 성공





# 메타마스크 설치하기

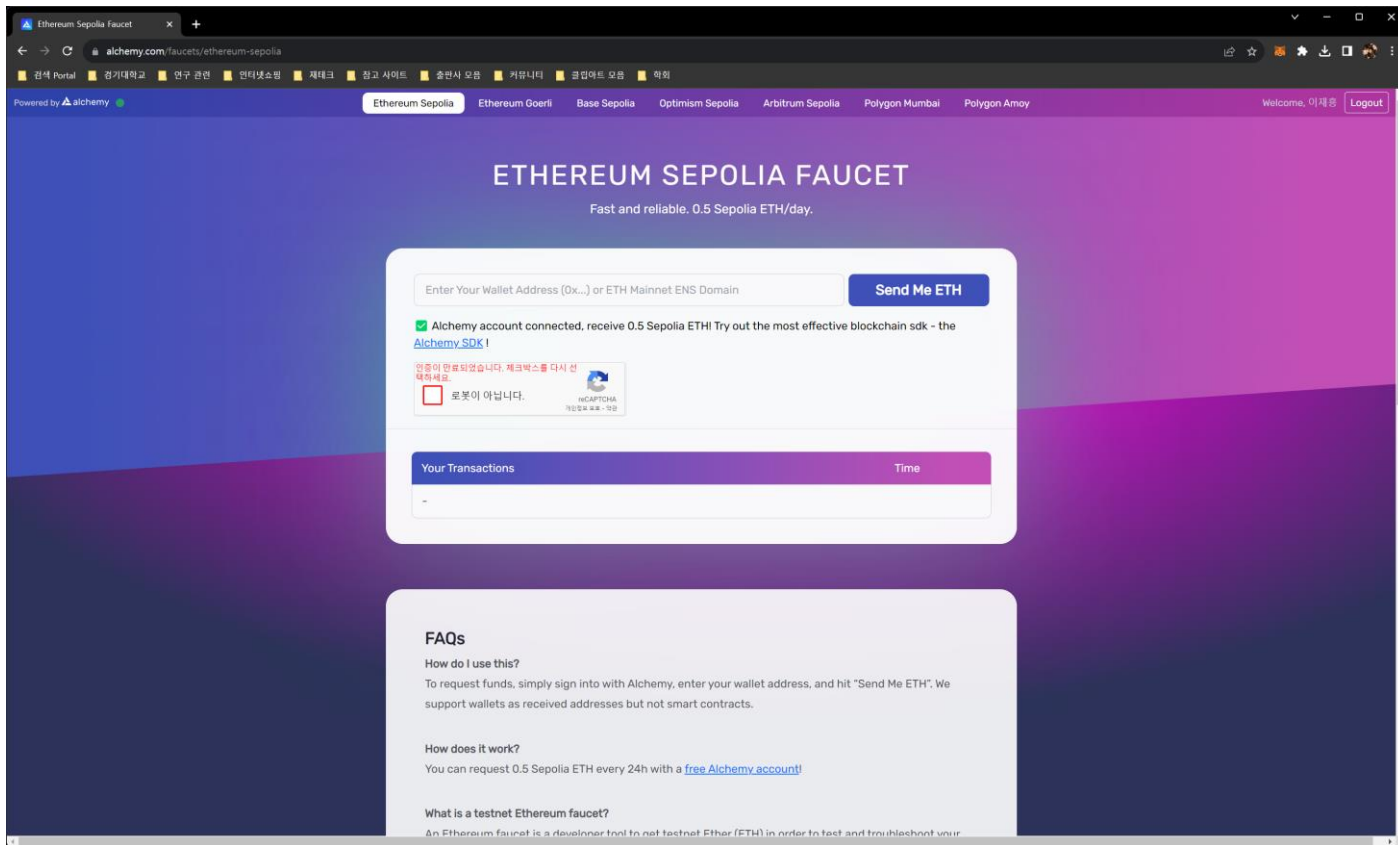
- 네트워크 바꾸기
  - 네트워크 선택
    - 테스트 네트워크 중 Sepolia로 변경





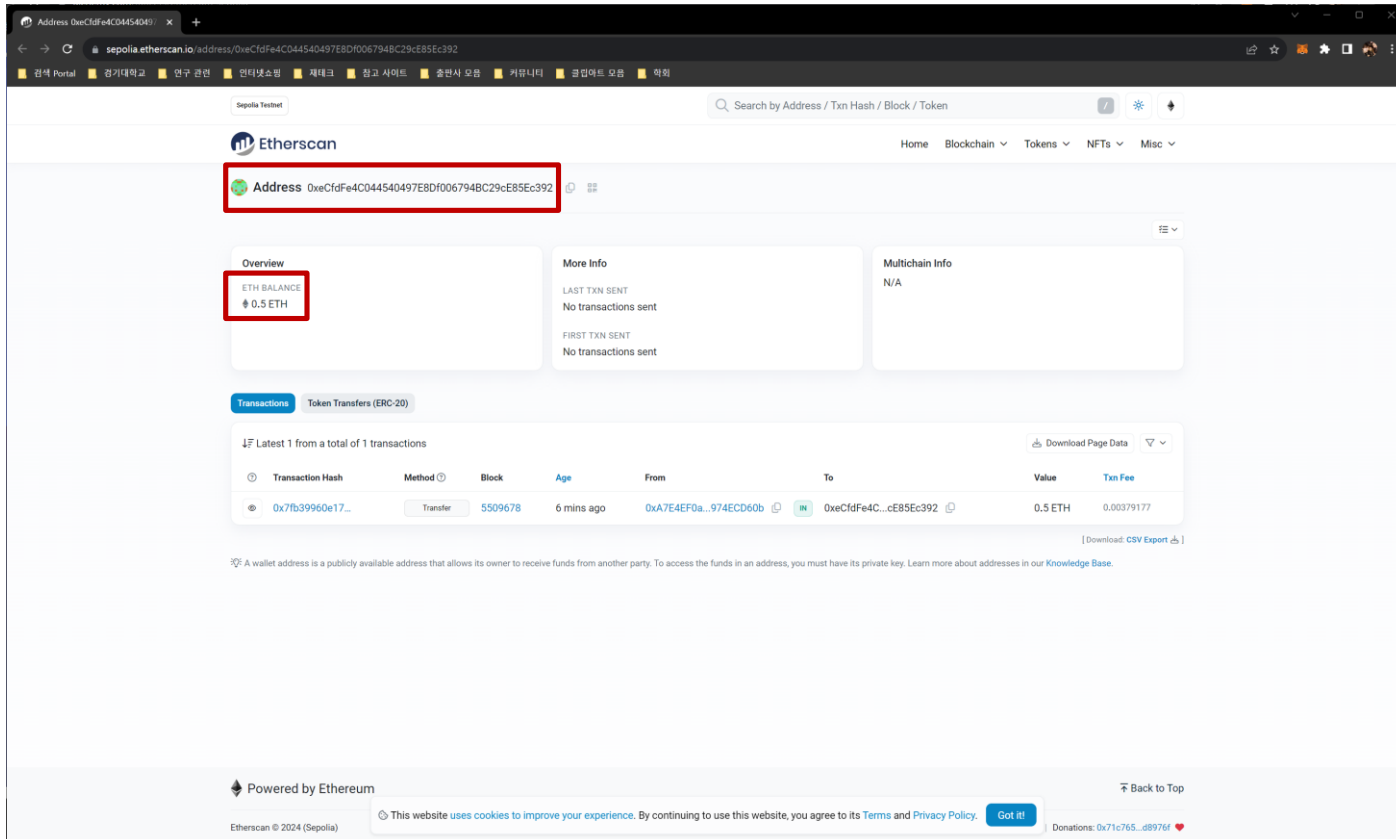
# 메타마스크 설치하기

- 테스트 이더 얻기 (from Ethereum Sepolia Faucet)
  - <https://www.alchemy.com/faucets/ethereum-sepolia>
  - 하루에 한 번 0.5 SepoliaETH를 받을 수 있음 (회원 가입 필요)



# 메타마스크 설치하기

- 테스트 이더 얻기 (from Ethereum Sepolia Faucet)
  - Etherscan에서 결과 확인하기 (이더리움 주소)
    - [https://sepolia.etherscan.io/address/이더리움\\_주소](https://sepolia.etherscan.io/address/이더리움_주소)



The screenshot shows the Etherscan Sepolia Testnet interface. At the top, the address `0xeCfdFe4C044540497E8Df006794BC29cE85Ec392` is highlighted with a red box. Below the address, the 'Overview' section shows an 'ETH BALANCE' of `0.5 ETH`, also highlighted with a red box. The 'Transactions' section shows a single transaction with a value of `0.5 ETH`. The page includes a search bar, navigation links (Home, Blockchain, Tokens, NFTs, Misc), and a footer with 'Powered by Ethereum' and a cookie notice.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x7fb39960e17...	Transfer	5509678	6 mins ago	0xA7E4EF0a...974ECD60b	0xeCfdFe4C...e85Ec392	0.5 ETH	0.00379177



# 메타마스크 설치하기

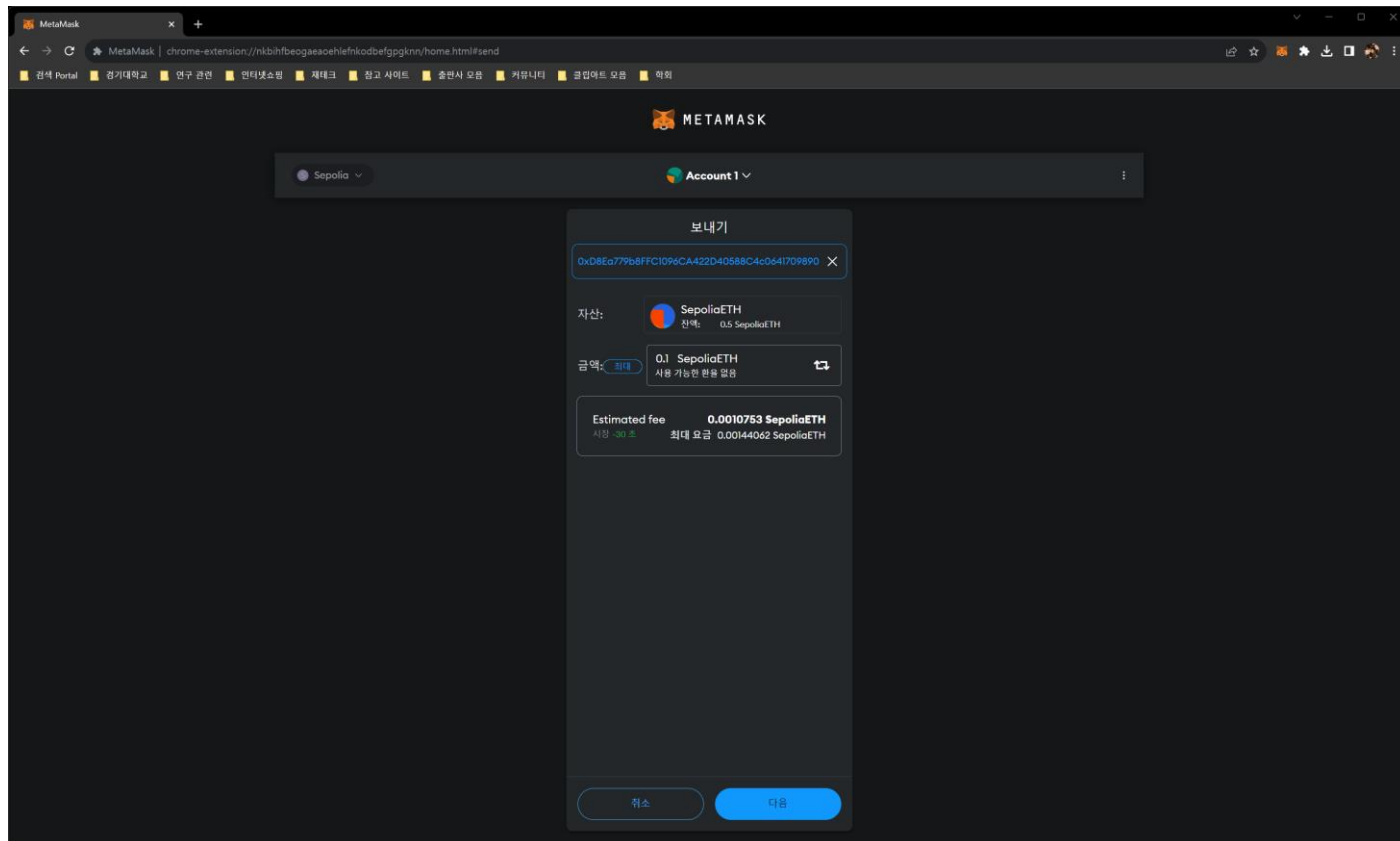
- 테스트 이더 얻기 (from Ethereum Sepolia Faucet)
  - Etherscan에서 결과 확인하기 (트랜잭션 해시)
    - [https://sepolia.etherscan.io/tx/트랙잭션\\_해시](https://sepolia.etherscan.io/tx/트랙잭션_해시)

The screenshot shows the Etherscan Sepolia Testnet transaction details page. The transaction hash is 0x7fb39960e177ca75a4ca59ba5eb669ae95c79a5d8c0c44d8c146ce76a55f74f0. The status is 'Success'. The transaction is from 0xA7E4EF0a9e15bDEF215E2ed87AE050f974ECD60b to 0xcCfdF4C044540497E8DF006794BC29cE85Ec392. The value is 0.5 ETH (\$0.00). The transaction fee is 0.00379177304478 ETH (\$0.00). The gas price is 180.56062118 Gwei (0.00000018056062118 ETH).

Field	Value
Transaction Hash	0x7fb39960e177ca75a4ca59ba5eb669ae95c79a5d8c0c44d8c146ce76a55f74f0
Status	Success
Block	5509678 (31 Block Confirmations)
Timestamp	7 mins ago (Mar-18-2024 06:46:36 AM +UTC)
From	0xA7E4EF0a9e15bDEF215E2ed87AE050f974ECD60b
To	0xcCfdF4C044540497E8DF006794BC29cE85Ec392
Value	0.5 ETH (\$0.00)
Transaction Fee	0.00379177304478 ETH (\$0.00)
Gas Price	180.56062118 Gwei (0.00000018056062118 ETH)

# 메타마스크 설치하기

- 메타마스크에서 이더 보내기 (to Ethereum Sepolia Faucet)
  - 아래 주소로 0.1 SepoliaETH 송금
    - 0xD8Ea779b8FFC1096CA422D40588C4c0641709890

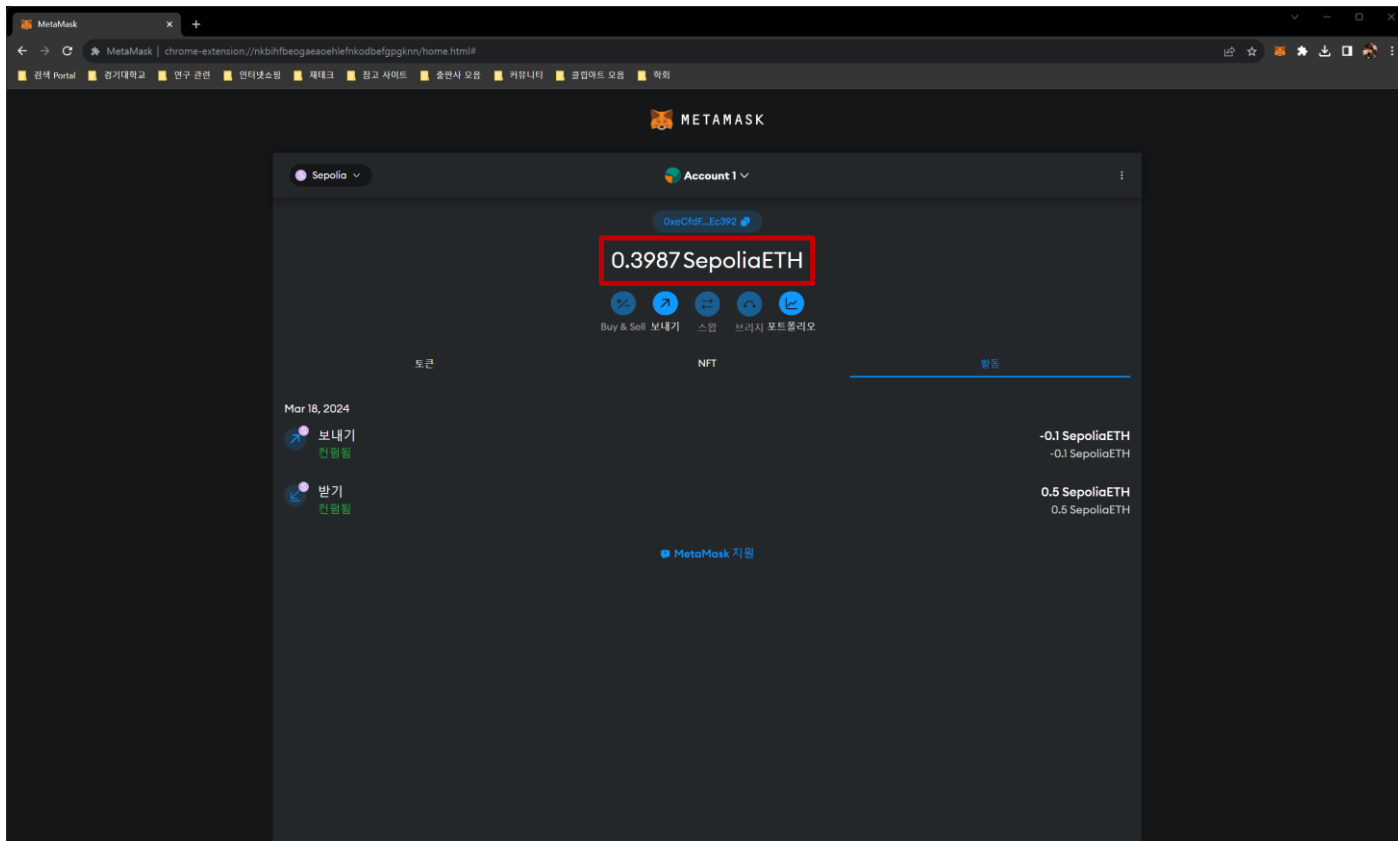






# 메타마스크 설치하기

- 메타마스크에서 이더 보내기 (to Ethereum Sepolia Faucet)
  - 남은 이더가 0.4 SepoliaETH가 아닌 이유는?
    - 가스 비용





## 월드 컴퓨터 소개

- 탈중앙화된 월드 컴퓨터로서의 이더리움
  - 암호화폐 기능은 이더리움의 기능에 부차적인 것
    - 이더
      - 이더리움 가상 머신(Ethereum Virtual Machine, EVM)이라고 하는 에뮬레이트된 컴퓨터에서 실행되는 컴퓨터 프로그램인 스마트 컨트랙트(smart contract)를 실행하는데 사용되기 위한 것
  - EVM
    - 글로벌 싱글톤으로, 마치 전 세계에 걸친 단일 인스턴스 컴퓨터인 것처럼 작동하며 세상 어디에서나 실행됨
    - 이더리움 네트워크의 각 노드는 컨트랙트 실행을 확인하기 위해 EVM의 로컬 사본을 실행하고, 이더리움 블록체인은 트랜잭션과 스마트 컨트랙트를 처리할 때 월드 컴퓨터의 변화하는 상태(state)를 기록함



## 외부 소유 계정(EOA) 및 컨트랙트

- 외부 소유 계정(Externally Owned Account, EOA)
  - 메타마스크 지갑에서 생성한 계정 유형
  - 개인키가 있는 계정
    - 자금 또는 컨트랙트에 대한 접근을 제어할 수 있음



## 외부 소유 계정(EOA) 및 컨트랙트

- 컨트랙트 계정(contract account)
  - 단순한 EOA가 가질 수 없는 스마트 컨트랙트 코드를 가짐
  - 개인키가 없고, 스마트 컨트랙트 코드의 로직으로 제어
  - 스마트 컨트랙트 코드
    - 컨트랙트 계정 생성 시 이더리움 블록체인에 기록되고 EVM에 의해 실행되는 소프트웨어 프로그램



## 외부 소유 계정(EOA) 및 컨트랙트

- 컨트랙트 계정(contract account)
  - EOA와 마찬가지로 주소가 있으며, 이더를 보내고 받을 수 있음
  - 트랜잭션 목적지가 컨트랙트 주소일 때 트랜잭션과 트랜잭션 데이터를 입력으로 사용하여 컨트랙트가 EVM에서 실행됨(run)
  - 이더 외에도 트랜잭션에는 실행할 컨트랙트의 특정 함수와 해당 함수에 전달할 파라미터를 나타내는 데이터(data)가 포함될 수 있음
  - 이를 통해 트랜잭션은 컨트랙트 내의 함수를 호출(call)할 수 있음
  - 개인키가 없으므로 트랜잭션을 시작할 수는 없음
  - EOA만 트랜잭션을 시작(initiate)할 수 있지만, 컨트랙트는 복잡한 실행 경로를 구축하여 다른 컨트랙트를 호출해서 컨트랙트에 반응(react)할 수 있음



## 간단한 컨트랙트: 테스트 이더 Faucet

- Faucet을 구현하는 솔리디티 컨트랙트
  - Faucet.sol

```
// SPDX-License-Identifier: CC-BY-SA-4.0

// Version of Solidity compiler this program was written for
pragma solidity 0.8.24;

// Our first contract is a faucet!
contract Faucet {
    // Accept any incoming amount
    receive() external payable {}

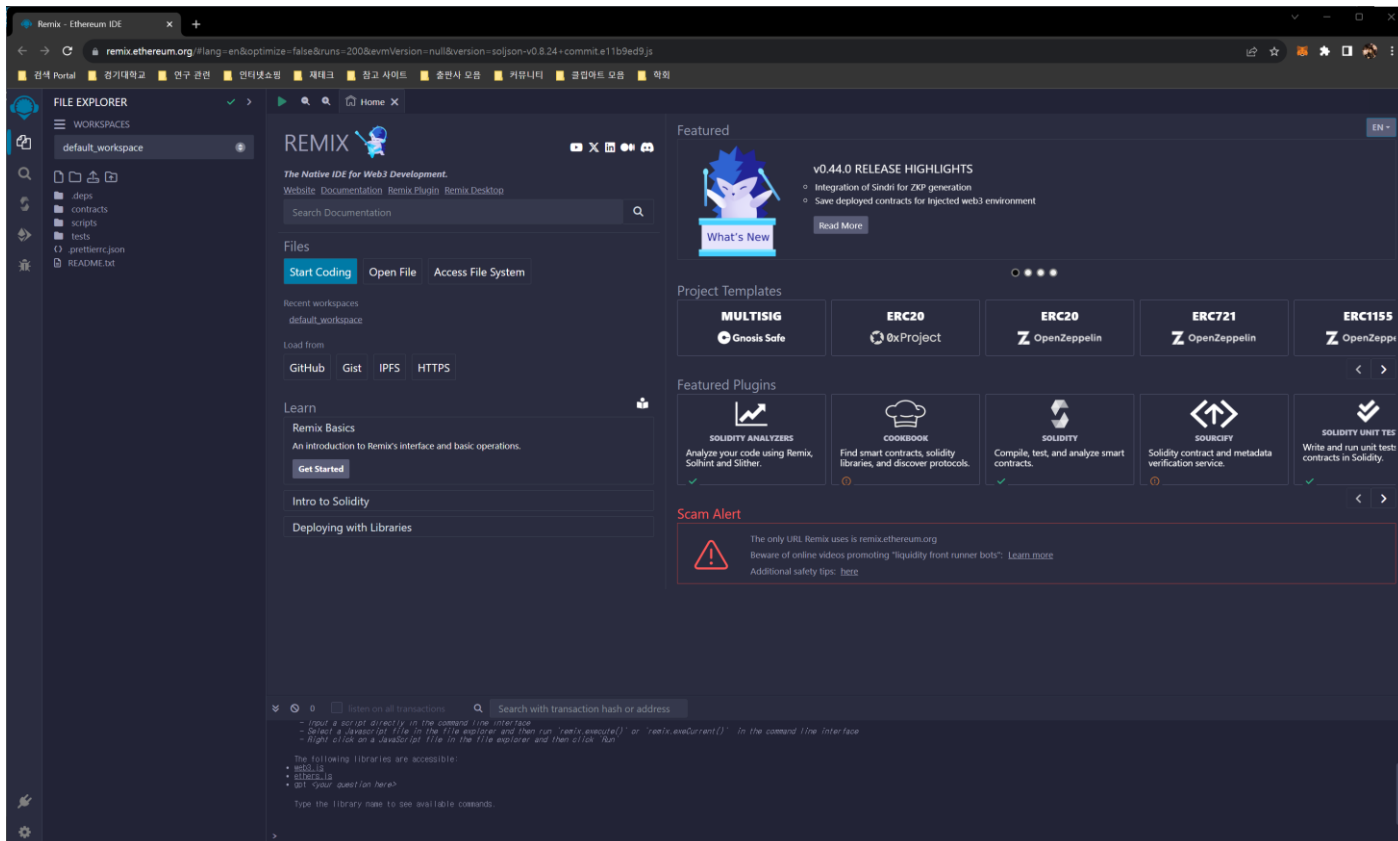
    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {
        // Limit withdrawal amount
        require(withdraw_amount <= 1000000000000000000);

        // Send the amount to the address that requested it
        payable(msg.sender).transfer(withdraw_amount);
    }
}
```



# Faucet 컨트랙트 컴파일

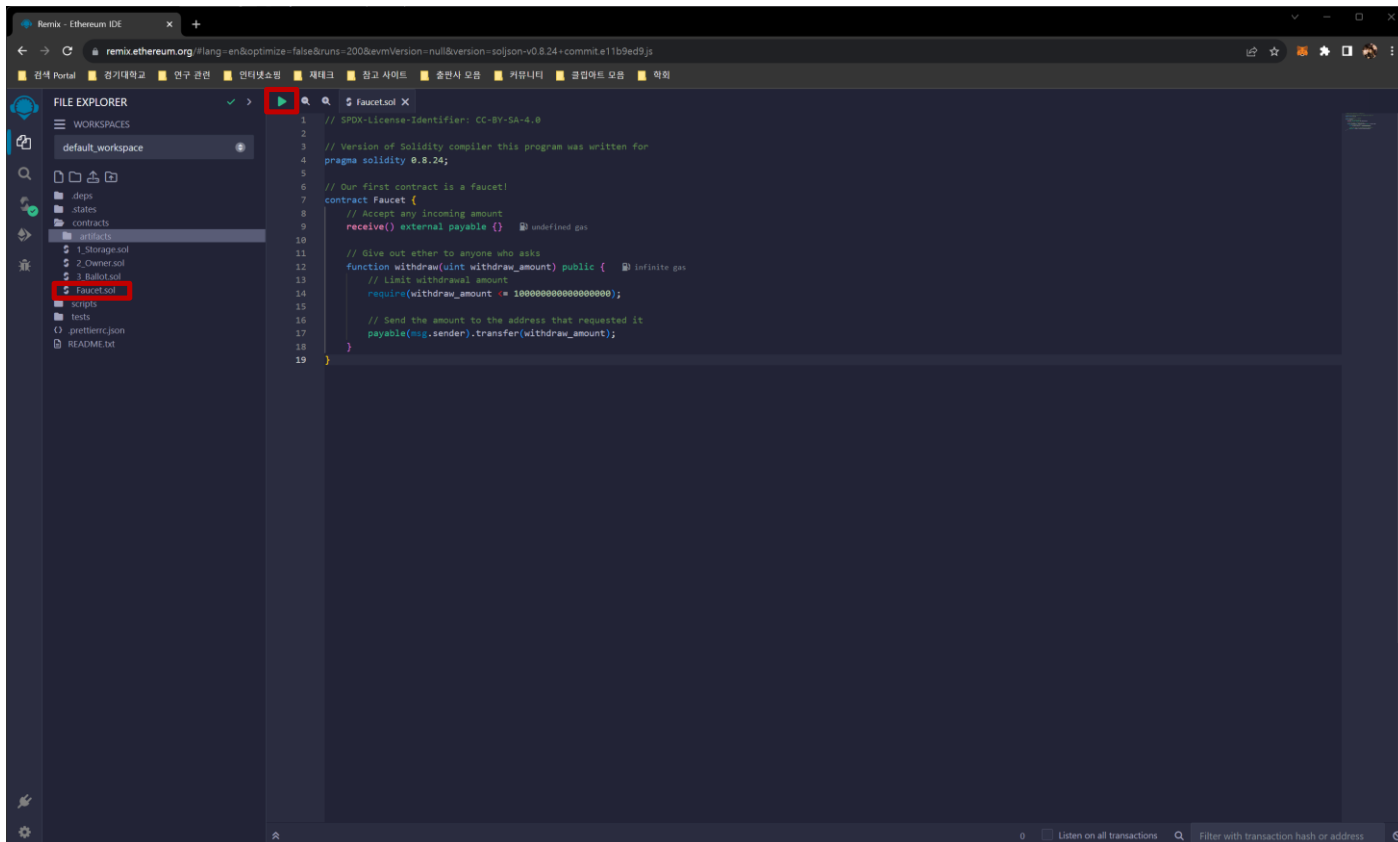
- 리믹스(Remix) IDE
  - 브라우저에서 솔리디티를 이용하여 스마트 컨트랙트를 개발하도록 도와주는 IDE
  - <https://remix.ethereum.org>





# Faucet 컨트랙트 컴파일

- 리믹스(Remix) IDE
  - contracts 폴더 밑에 Faucet.sol 작성 후 컴파일
  - 솔리디티 버전 확인 필요







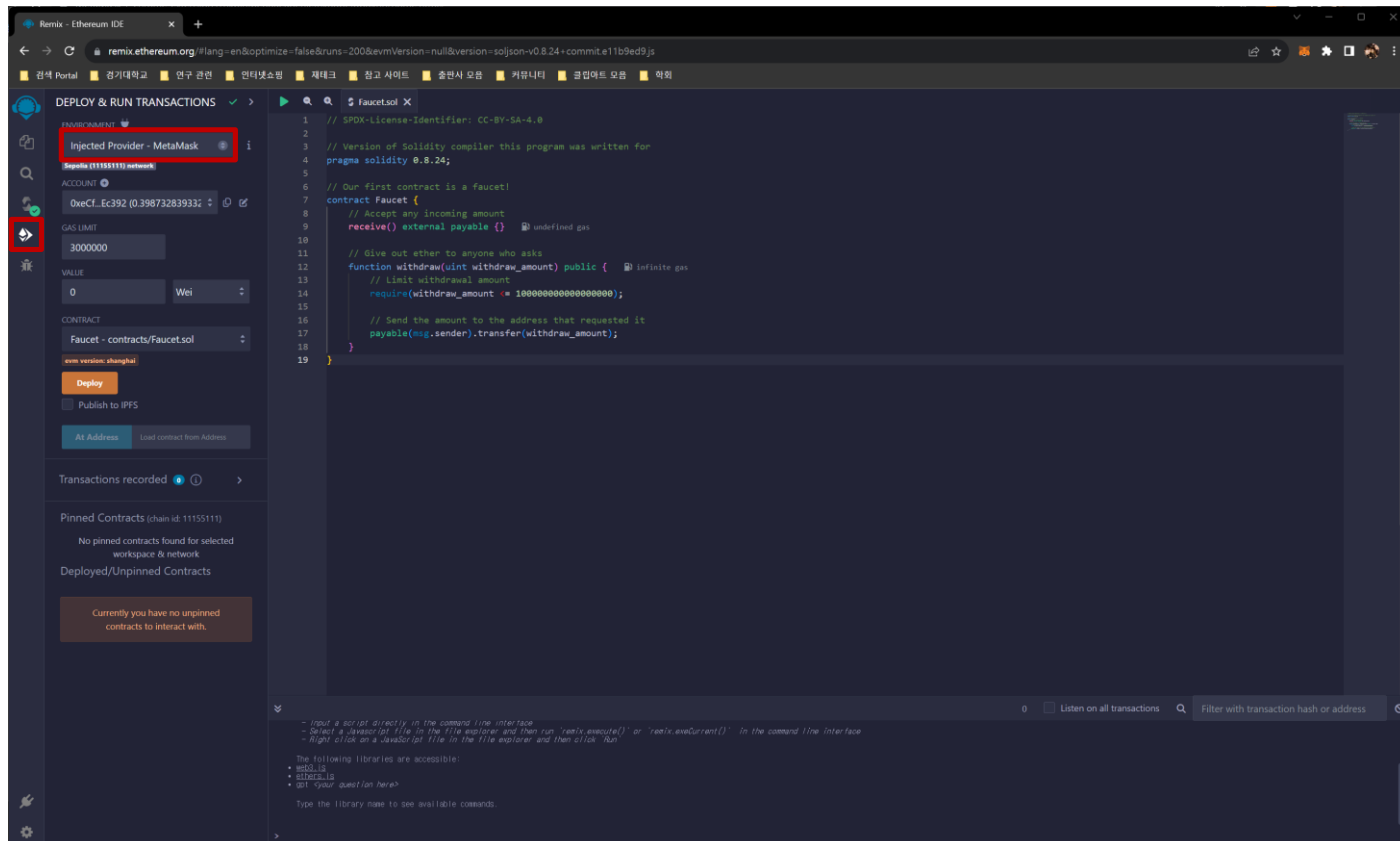
## Faucet 컨트랙트 컴파일

- 리믹스(Remix) IDE
  - 컴파일 결과 바이트 코드 (Faucet.json)

```
PUSH1 0x80 PUSH1 0x40 MSTORE CALLVALUE DUP1 ISZERO PUSH2 0xF JUMPI PUSH0 DUP1 REVERT  
JUMPDEST POP PUSH2 0x147 DUP1 PUSH2 0x1D PUSH0 CODECOPY PUSH0 RETURN INVALID PUSH1 0x80  
PUSH1 0x40 MSTORE PUSH1 0x4 CALLDATASIZE LT PUSH2 0x21 JUMPI PUSH0 CALLDATALOAD PUSH1 0xE0  
SHR DUP1 PUSH4 0x2E1A7D4D EQ PUSH2 0x2C JUMPI PUSH2 0x28 JUMP JUMPDEST CALLDATASIZE PUSH2  
0x28 JUMPI STOP JUMPDEST PUSH0 DUP1 REVERT JUMPDEST CALLVALUE DUP1 ISZERO PUSH2 0x37  
JUMPI PUSH0 DUP1 REVERT JUMPDEST POP PUSH2 0x52 PUSH1 0x4 DUP1 CALLDATASIZE SUB DUP2 ADD  
SWAP1 PUSH2 0x4D SWAP2 SWAP1 PUSH2 0xE6 JUMP JUMPDEST PUSH2 0x54 JUMP JUMPDEST STOP  
JUMPDEST PUSH8 0x16345785D8A0000 DUP2 GT ISZERO PUSH2 0x68 JUMPI PUSH0 DUP1 REVERT  
JUMPDEST CALLER PUSH20 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF AND PUSH2 0x8FC DUP3  
SWAP1 DUP2 ISZERO MUL SWAP1 PUSH1 0x40 MLOAD PUSH0 PUSH1 0x40 MLOAD DUP1 DUP4 SUB DUP2  
DUP6 DUP9 DUP9 CALL SWAP4 POP POP POP POP ISZERO DUP1 ISZERO PUSH2 0xAB JUMPI  
RETURN DATASIZE PUSH0 DUP1 RETURN DATACOPY RETURN DATASIZE PUSH0 REVERT JUMPDEST POP  
POP JUMP JUMPDEST PUSH0 DUP1 REVERT JUMPDEST PUSH0 DUP2 SWAP1 POP SWAP2 SWAP1 POP  
JUMP JUMPDEST PUSH2 0xC5 DUP2 PUSH2 0xB3 JUMP JUMPDEST DUP2 EQ PUSH2 0xCF JUMPI PUSH0  
DUP1 REVERT JUMPDEST POP JUMP JUMPDEST PUSH0 DUP2 CALLDATALOAD SWAP1 POP PUSH2 0xE0  
DUP2 PUSH2 0xBC JUMP JUMPDEST SWAP3 SWAP2 POP POP JUMP JUMPDEST PUSH0 PUSH1 0x20 DUP3  
DUP5 SUB SLT ISZERO PUSH2 0xFB JUMPI PUSH2 0xFA PUSH2 0xAF JUMP JUMPDEST JUMPDEST PUSH0  
PUSH2 0x108 DUP5 DUP3 DUP6 ADD PUSH2 0xD2 JUMP JUMPDEST SWAP2 POP POP SWAP3 SWAP2 POP  
POP JUMP INVALID LOG2 PUSH5 0x6970667358 0x22 SLT KECCAK256 MULMOD CODECOPY 0xD0 PUSH7  
0xDDC52AB0A0ED3E 0xD9 0xB4 0xB5 OR DUP14 0xAE POP 0x2F DUP15 PUSH20  
0x3DD81CB48E38DFC11B925164736F6C6343000818 STOP CALLER
```

# 블록체인에 컨트랙트 생성하기

- 리믹스(Remix) IDE
  - Deploy & run transactions 탭
    - Environment를 Injected Provider - MetaMask로 선택





# 블록체인에 컨트랙트 생성하기

- 리믹스(Remix) IDE
  - Deploy & run transactions 탭
    - Deploy 결과

The screenshot shows the Etherscan Sepolia Testnet transaction details page. The transaction hash is 0xb26833f8a762386174c815b6a9ab55fa775663e558378e20cad719da5264fed3. The status is 'Success' with 1 block confirmation. The transaction action is a 'Call' to the contract 0xc2615dcd81e29c2eb94f9abaf430788c6372b008. The 'To' field is highlighted with a red box, showing the contract address and the text '[ 0xc2615dcd81e29c2eb94f9abaf430788c6372b008 Created ]'. The value is 0 ETH (\$0.00) and the gas price is 59.091752959 Gwei.

Transaction Details

[ This is a Sepolia Testnet transaction only ]

Transaction Hash: 0xb26833f8a762386174c815b6a9ab55fa775663e558378e20cad719da5264fed3

Status: Success

Block: 5509750 1 Block Confirmation

Timestamp: 31 secs ago (Mar-18-2024 07:03:00 AM +UTC)

Transaction Action: Call 0xc60806040 Method by 0xcCfdFe4C...cE85Ec392

From: 0xcCfdFe4C044540497E8Df006794BC29cE85Ec392

To: [ 0xc2615dcd81e29c2eb94f9abaf430788c6372b008 Created ]

Value: 0 ETH (\$0.00)

Transaction Fee: 0.007321409099867141 ETH (\$0.00)

Gas Price: 59.091752959 Gwei (0.000000059091752959 ETH)

More Details: Click to show more

Powered by Ethereum

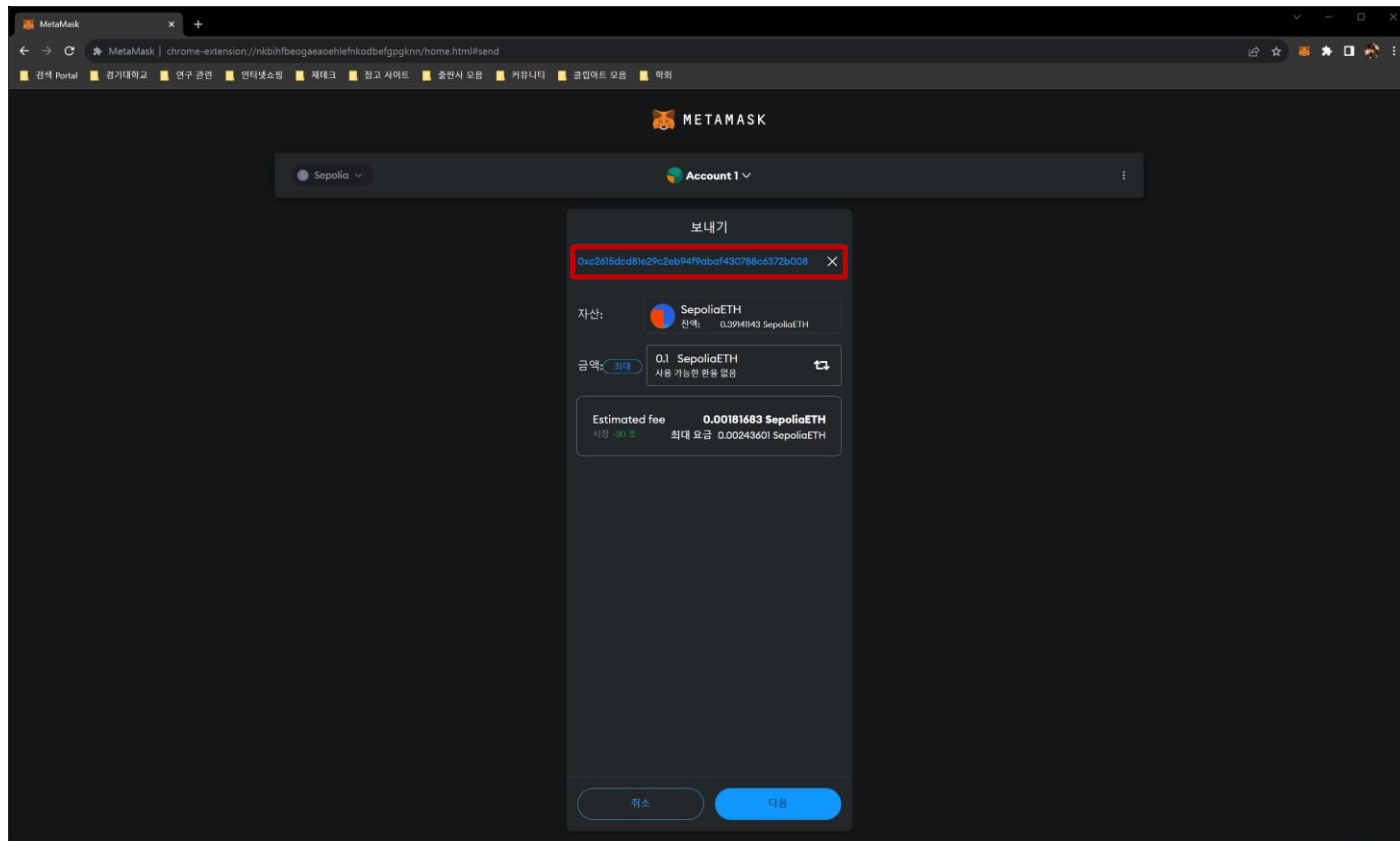
Etherscan © 2024 (Sepolia)

Terms & Privacy | Network Status | Donations: 0x71c765...d8976f



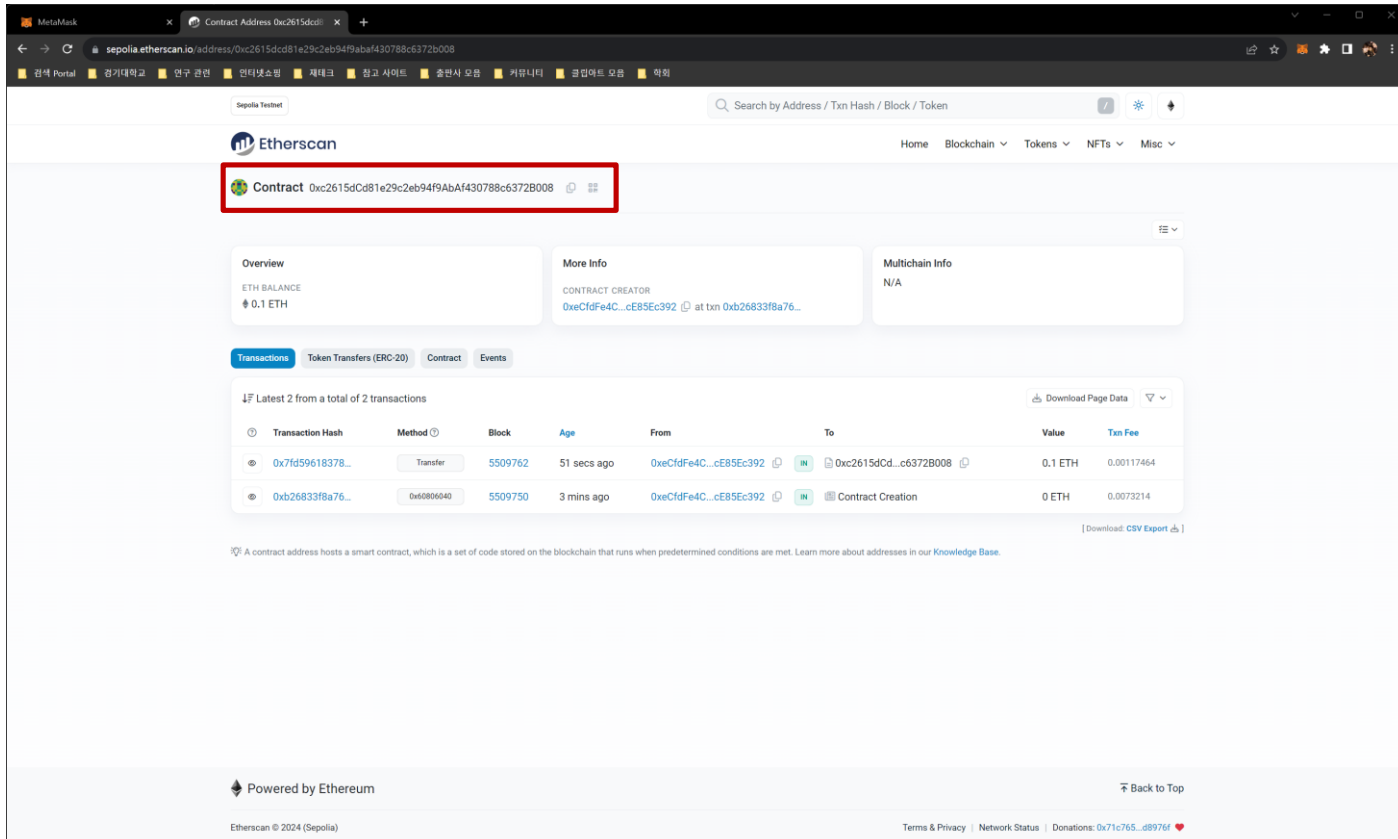
# 컨트랙트 사용하기

- 컨트랙트 자금 조달
  - 메타마스크를 통해 새로 생성된 컨트랙트에게 0.1 SepoliaETH 송금



# 컨트랙트 사용하기

- 컨트랙트 자금 조달
  - 송금 결과



The screenshot displays the Etherscan Sepolia Testnet interface. At the top, the search bar shows the contract address `0xc2615dCd81e29c2eb94f9AbAf430788c6372B008`, which is highlighted with a red box. Below the search bar, the page is divided into sections: Overview, More Info, and Multichain Info. The Overview section shows the ETH balance as 0.1 ETH. The More Info section lists the contract creator as `0xcfdFe4C...cE85Ec392`. The Transactions section shows two transactions: a transfer of 0.1 ETH and a contract creation. The table below details these transactions.

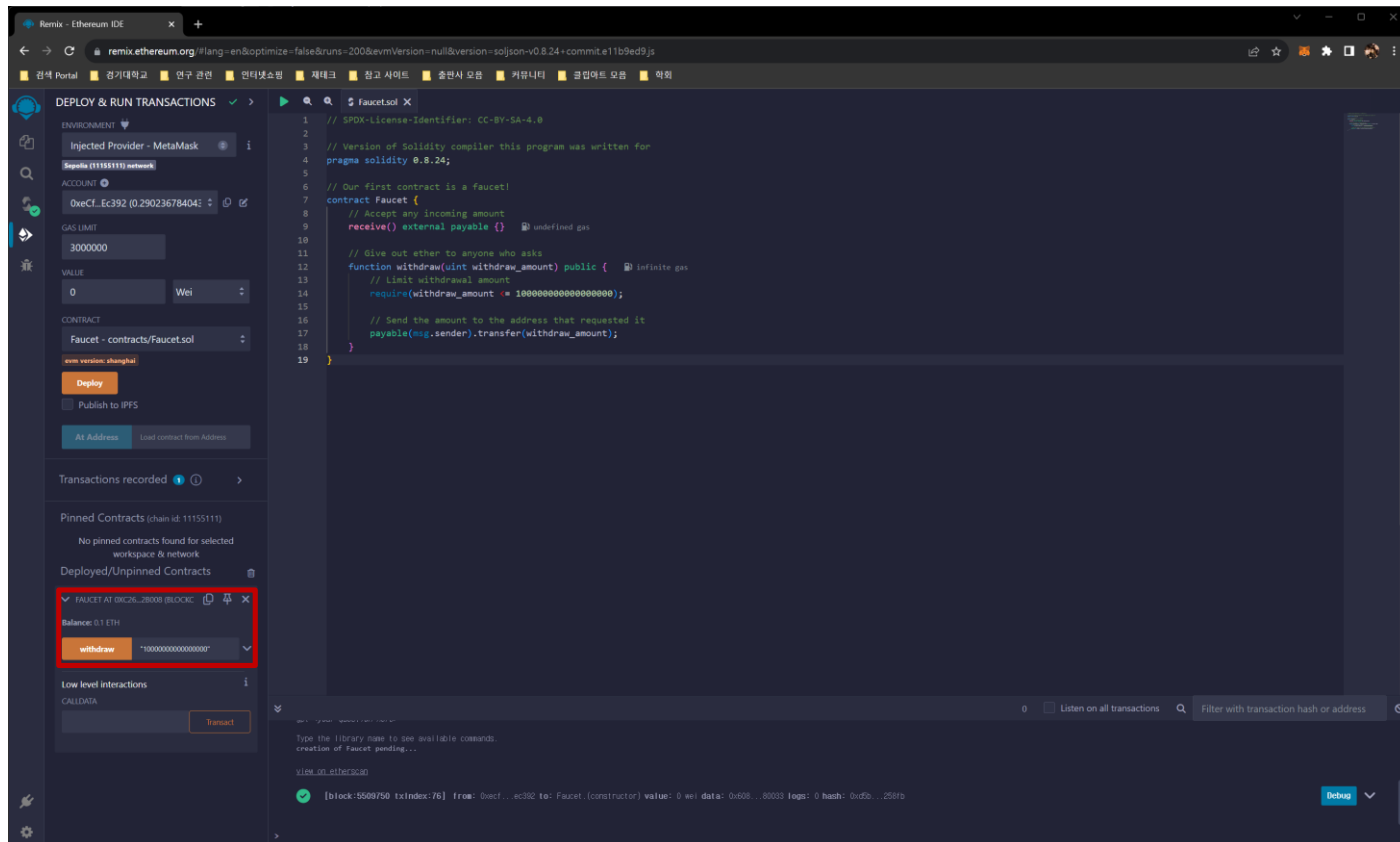
Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
<a href="#">0x71d59618378...</a>	Transfer	5509762	51 secs ago	<a href="#">0xcfdFe4C...cE85Ec392</a>	<a href="#">0xc2615dCd...c6372B008</a>	0.1 ETH	0.00117464
<a href="#">0xb26833f8a76...</a>	<code>0x60806040</code>	5509750	3 mins ago	<a href="#">0xcfdFe4C...cE85Ec392</a>	Contract Creation	0 ETH	0.0073214

Powered by Ethereum

Etherscan © 2024 (Sepolia)

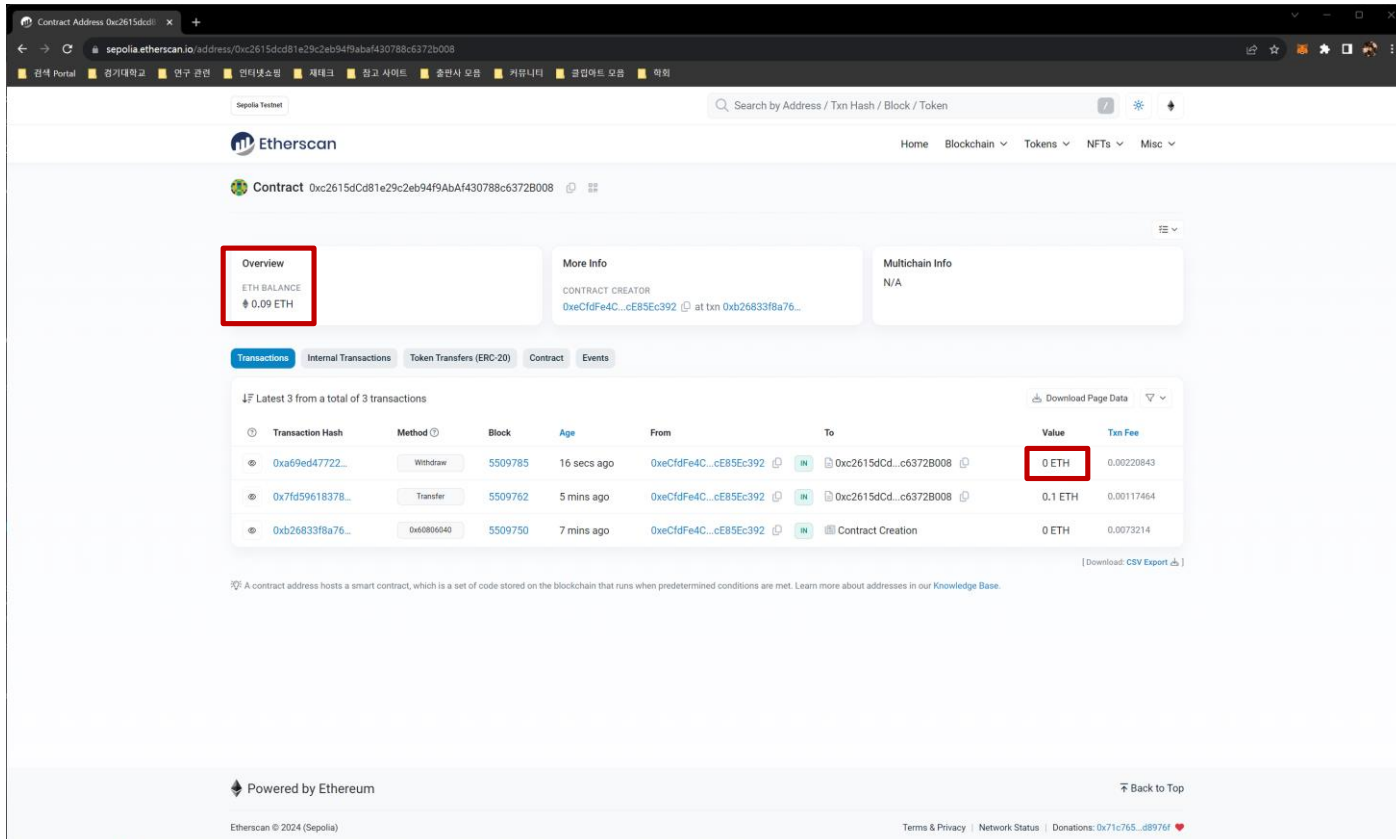
# 컨트랙트 사용하기

- 컨트랙트에서 출금
  - 컨트랙트에서 0.01 SepoliaETH를 withdraw 함수를 통해 인출
    - 0.01 SepoliaETH = 10,000,000,000,000,000 웨이



# 컨트랙트 사용하기

- 컨트랙트에서 출금
  - ETH BALANCE가 0.1 ETH에서 0.09 ETH로 바뀐 것을 확인
    - Value가 0.01 ETH가 아닌 0 ETH인 이유는?

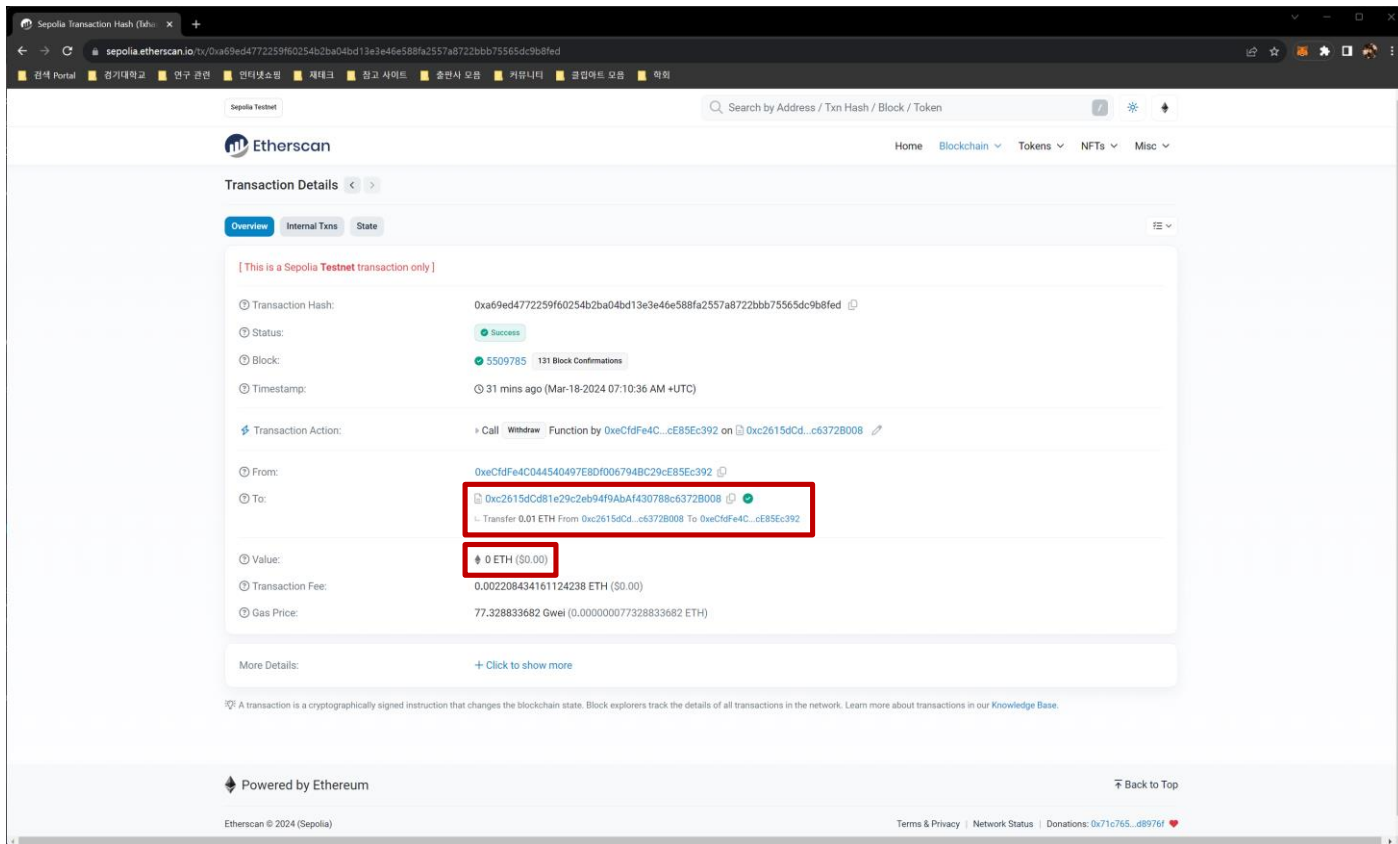


The screenshot shows the Etherscan Sepolia Testnet interface for a contract at address 0xc2615dcd81e29c2eb94f9AbA430788c6372B008. The 'Overview' tab is selected, showing an ETH BALANCE of 0.09 ETH. Below this, the 'Transactions' tab is active, displaying a table of the latest 3 transactions. The first transaction is a 'Withdraw' of 0.01 ETH, which is highlighted with a red box. The second transaction is a 'Transfer' of 0.1 ETH, and the third is a 'Contract Creation' with a value of 0 ETH, also highlighted with a red box. The table columns include Transaction Hash, Method, Block, Age, From, To, Value, and Txn Fee.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0xa69ed47722...	Withdraw	5509785	16 secs ago	0xeCfdFe4C...cE85Ec392	0xc2615dCd...c6372B008	0.01 ETH	0.00220843
0x7fd59618378...	Transfer	5509762	5 mins ago	0xeCfdFe4C...cE85Ec392	0xc2615dCd...c6372B008	0.1 ETH	0.00117464
0xb26833f8a76...	Contract Creation	5509750	7 mins ago	0xeCfdFe4C...cE85Ec392	0xc2615dCd...c6372B008	0 ETH	0.0073214

# 컨트랙트 사용하기

- 컨트랙트에서 출금
  - Internal Transactions
    - 0.01 ETH 전송은 컨트랙트 코드에서 시작되었기 때문에 내부 트랜잭션임



The screenshot shows the Etherscan Sepolia Testnet interface. The transaction details are as follows:

- Transaction Hash:** 0xa69ed4772259f60254b2ba04bd13e3e46e588fa2557a8722bbb75565dc9b8fed
- Status:** Success
- Block:** 5509785 (131 Block Confirmations)
- Timestamp:** 31 mins ago (Mar-18-2024 07:10:36 AM +UTC)
- Transaction Action:** Call Withdraw Function by 0xc6dfe4c...cE85Ec392 on 0xc2615dCd...c6372B008
- From:** 0xc6dfe4c044540497E8Df006794BC29cE85Ec392
- To:** 0xc2615dCd91e29c2eb94f9AbA43078bc6372B008 (Transfer 0.01 ETH From 0xc6dfe4c...cE85Ec392 To 0xc2615dCd...c6372B008)
- Value:** 0 ETH (\$0.00)
- Transaction Fee:** 0.002208434161124238 ETH (\$0.00)
- Gas Price:** 77.328833682 Gwei (0.000000077328833682 ETH)

More Details: [Click to show more](#)

Powered by Ethereum

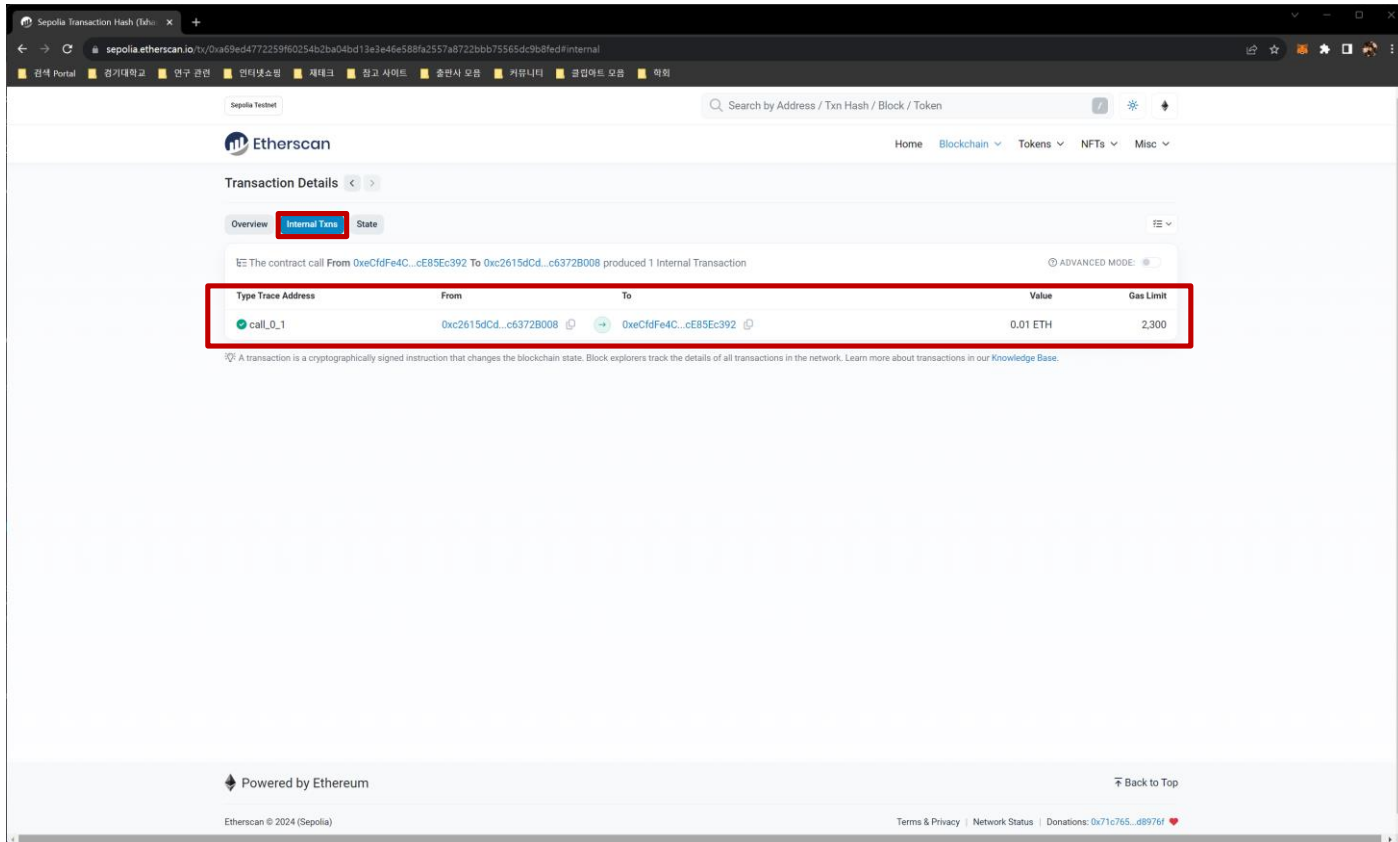
Etherscan © 2024 (Sepolia)

Terms & Privacy | Network Status | Donations: 0x71c765...d8976f



# 컨트랙트 사용하기

- 컨트랙트에서 출금
  - Internal Transactions
    - 0.01 ETH 전송은 컨트랙트 코드에서 시작되었기 때문에 내부 트랜잭션임



The screenshot shows the Etherscan Sepolia Testnet interface. The transaction hash is 0xa69ed477225960254b2ba04bd13e3e46e588fa2557a8722bbb75565dc9b8fedfinternal. The transaction details page is open, showing the 'Internal Transactions' tab. A message states: "The contract call From 0xcCfdFe4C...cE85Ec392 To 0xc2615dCd...c6372B008 produced 1 Internal Transaction". Below this, a table lists the internal transaction:

Type	Trace Address	From	To	Value	Gas Limit
call_0_1		0xc2615dCd...c6372B008	0xcCfdFe4C...cE85Ec392	0.01 ETH	2,300

At the bottom of the page, it says "Powered by Ethereum" and "Etherscan © 2024 (Sepolia)".

