



# 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



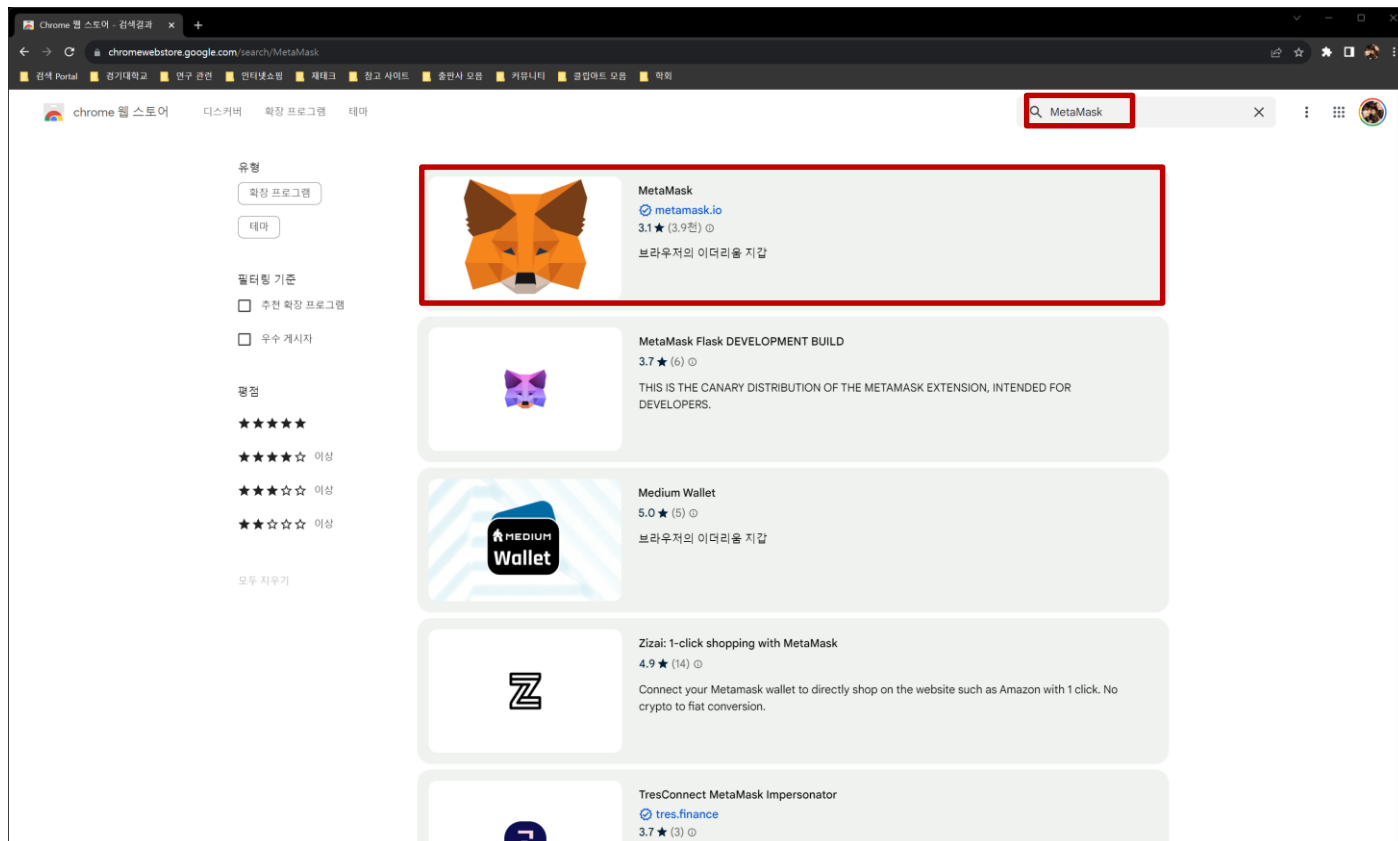
## 통제와 책임

- 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

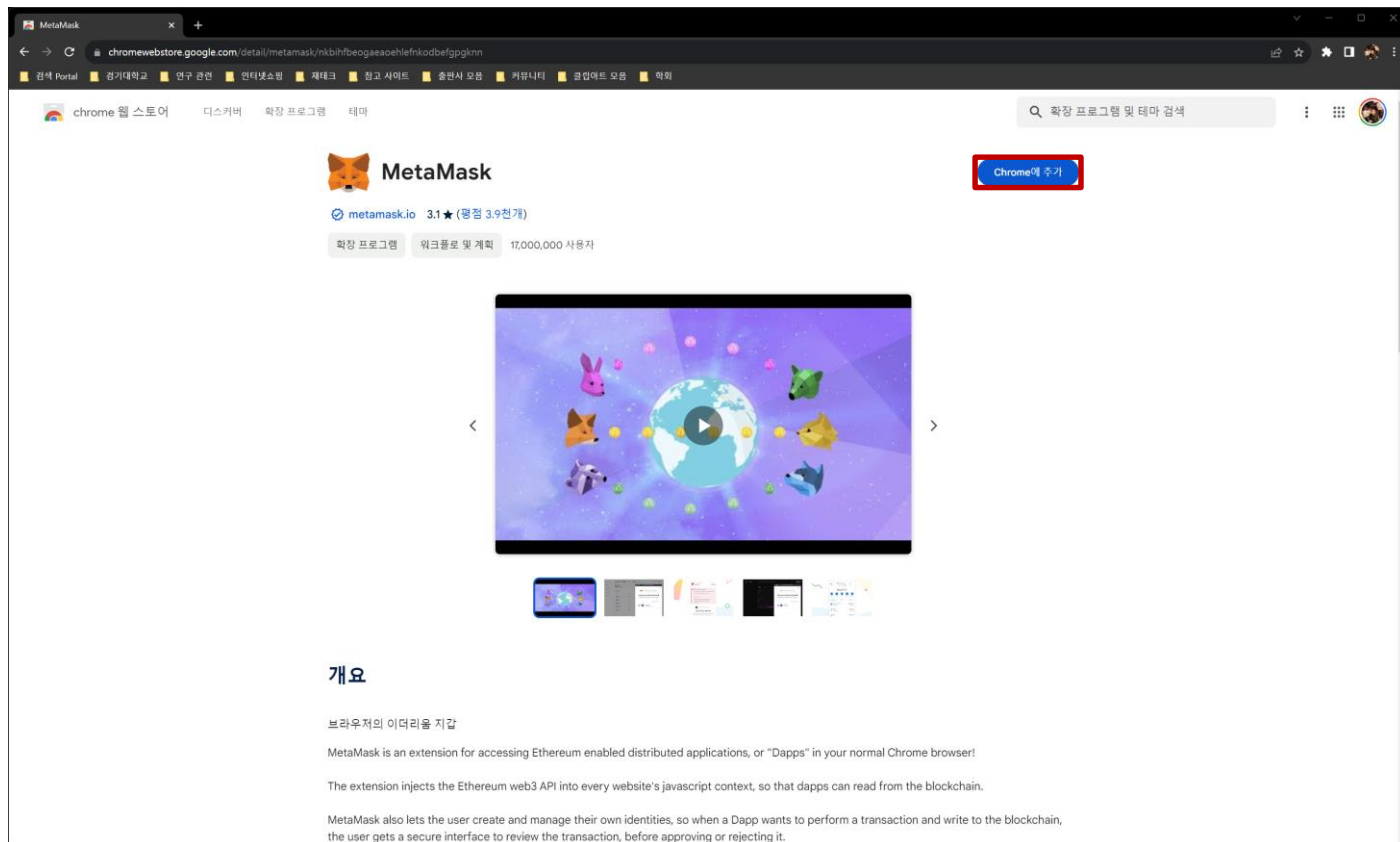
- 메타마스크 설치 과정

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



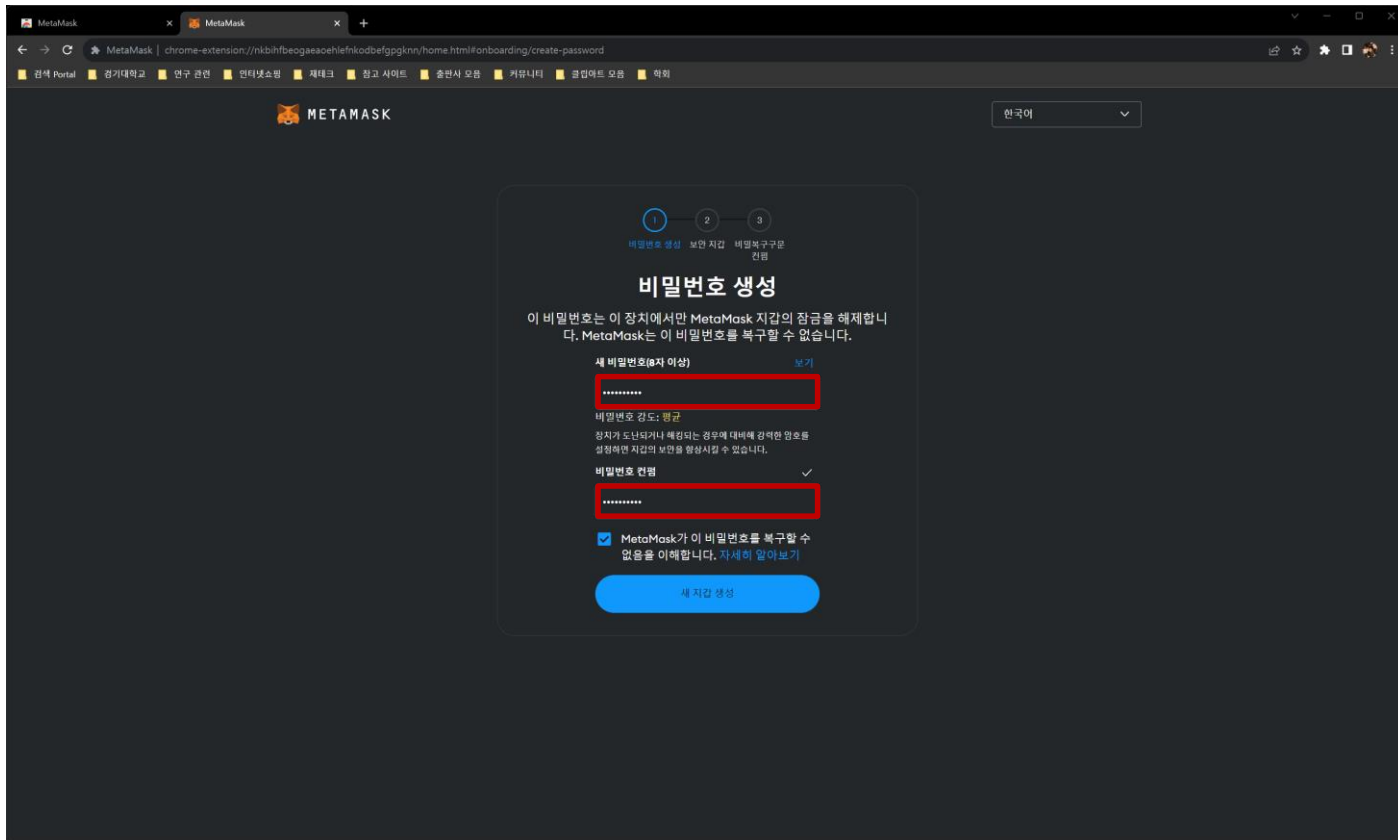
# 메타마스크 설치하기

- 메타마스크 설치 과정
  - ‘Chrome에 추가’ 클릭하여 설치



# 메타마스크 설치하기

- 지갑 만들기
  - 이용약관 동의
  - 비밀번호 생성

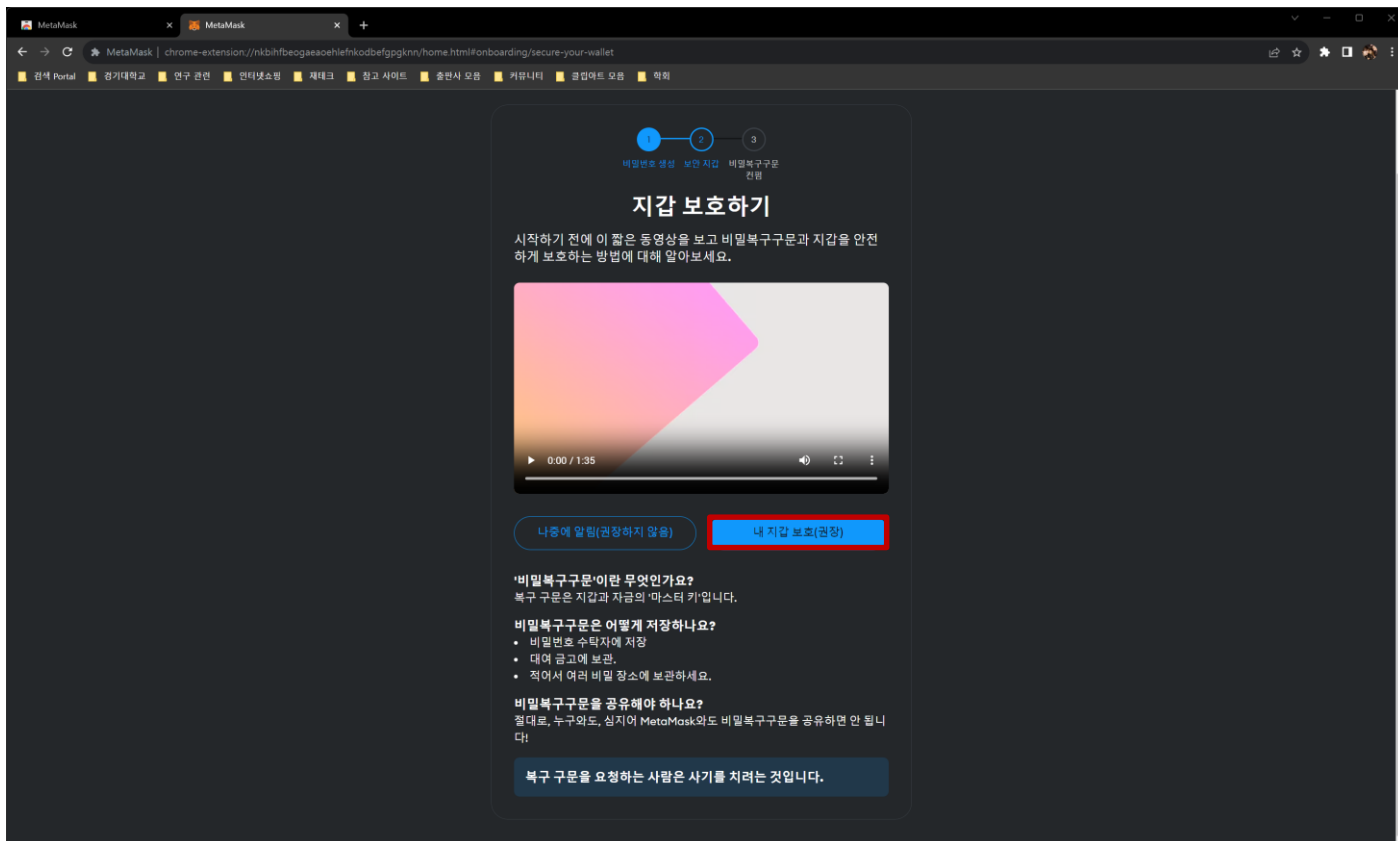


The screenshot shows the MetaMask onboarding interface in a web browser. The page title is "비밀번호 생성" (Create Password). It features a progress indicator at the top with three steps: 1. 비밀번호 생성 (Create Password), 2. 보안 지갑 (Secure Wallet), and 3. 비밀번호 복구구분 (Recovery Phrase). The main text explains that the password is for device access and cannot be recovered. There are two input fields: "새 비밀번호(8자 이상)" (New Password, 8+ characters) and "비밀번호 확인" (Confirm Password), both highlighted with red boxes. A checkbox at the bottom indicates agreement with the terms. A blue button at the bottom says "새 지갑 생성" (Create New Wallet).



# 메타마스크 설치하기

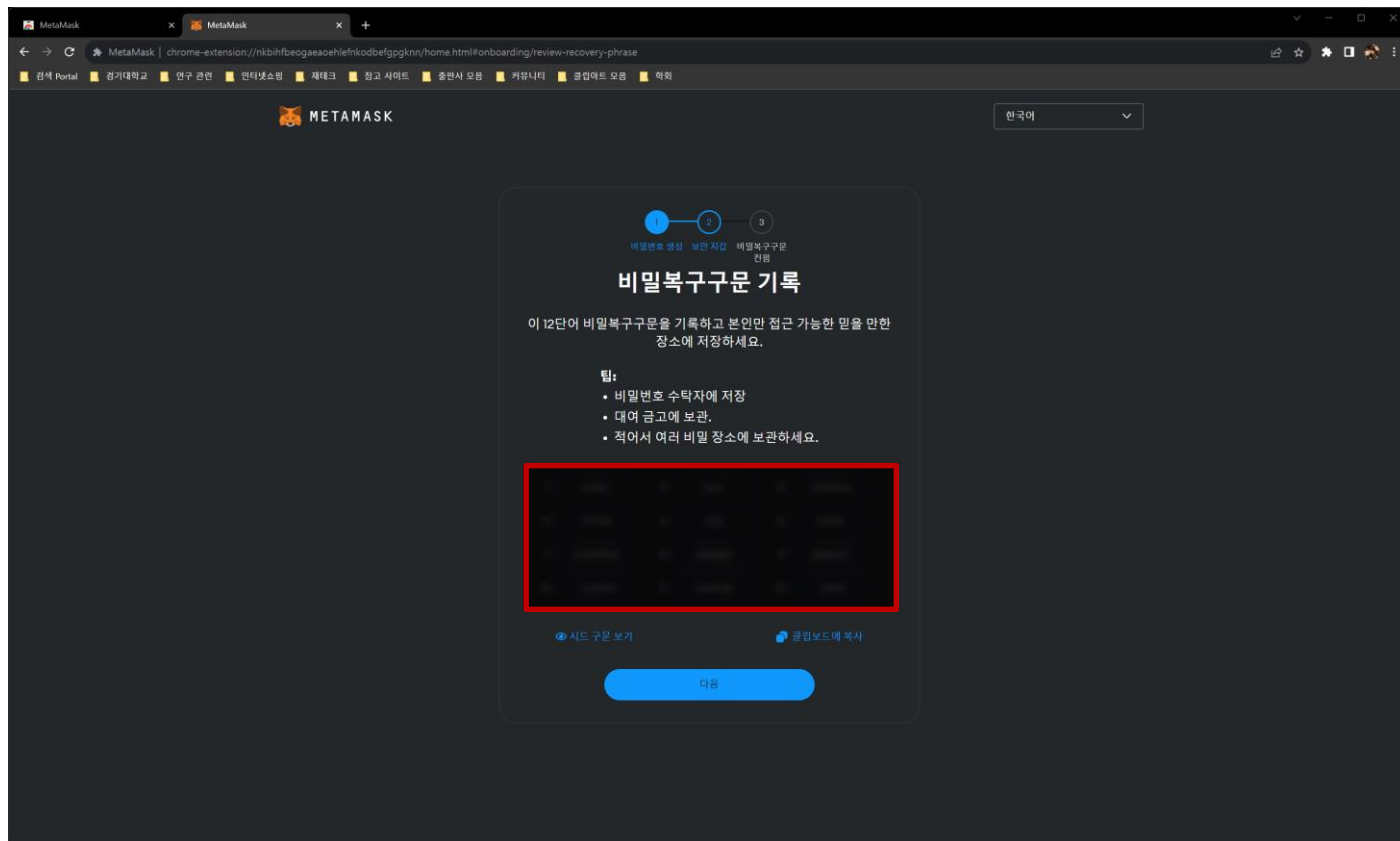
- 지갑 만들기
  - 지갑 보호하기
    - 내 지갑 보호(권장) 선택





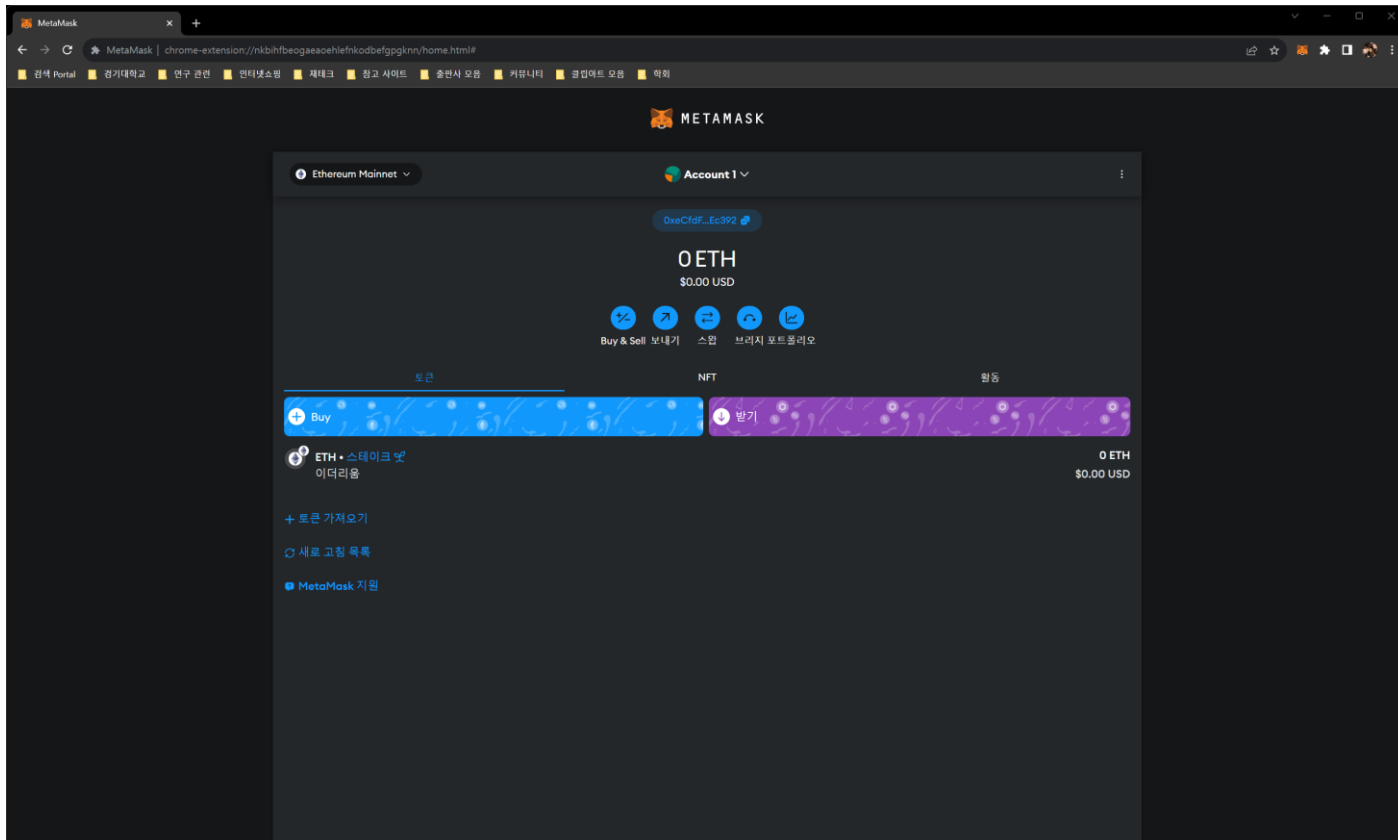
# 메타마스크 설치하기

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



# 메타마스크 설치하기

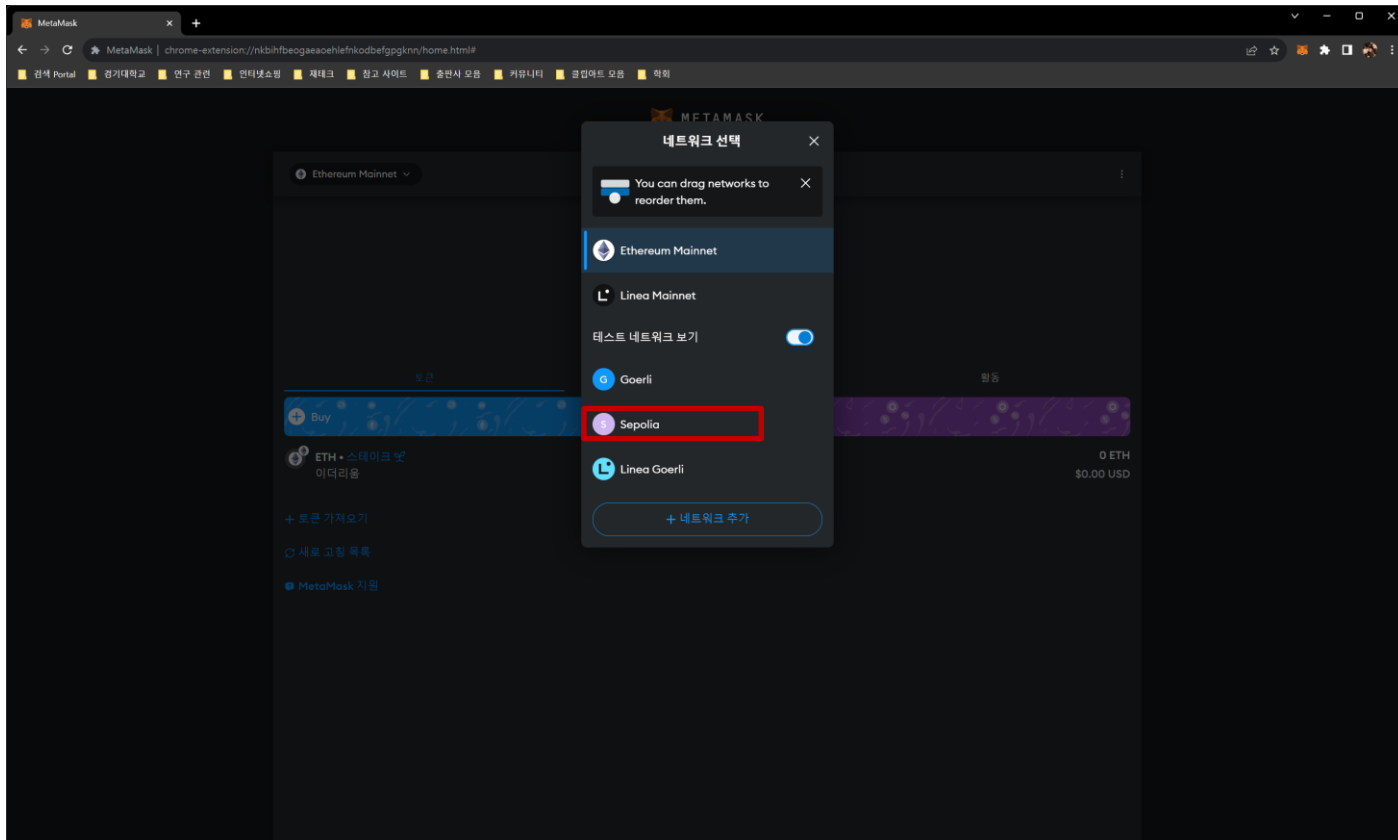
- 지갑 만들기
  - 비밀복구구문 컨펌
  - 지갑 생성 성공





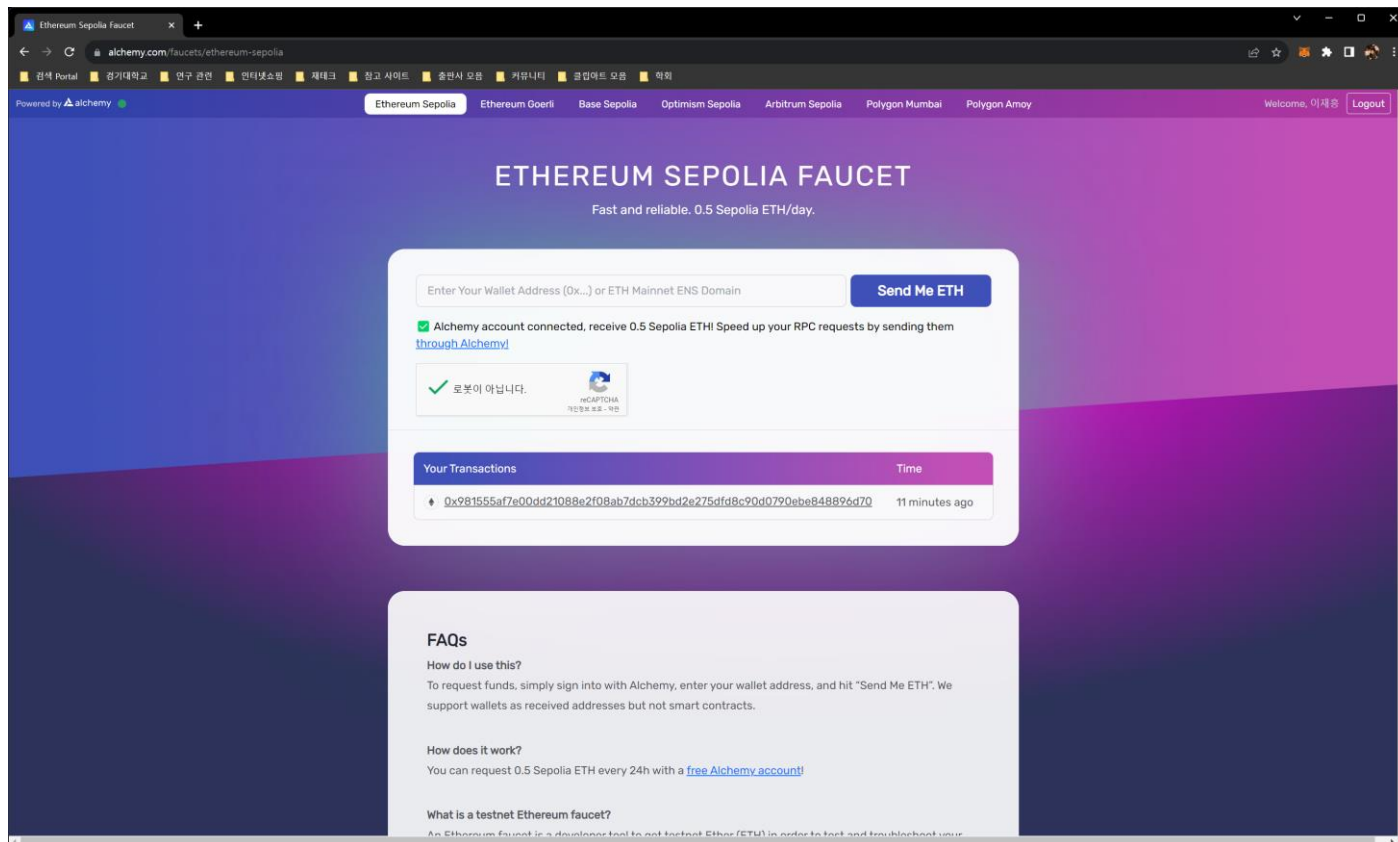
# 메타마스크 설치하기

- 네트워크 바꾸기
  - 사용 가능 네트워크
    - 테스트 네트워크 중 Sepolia로 변경



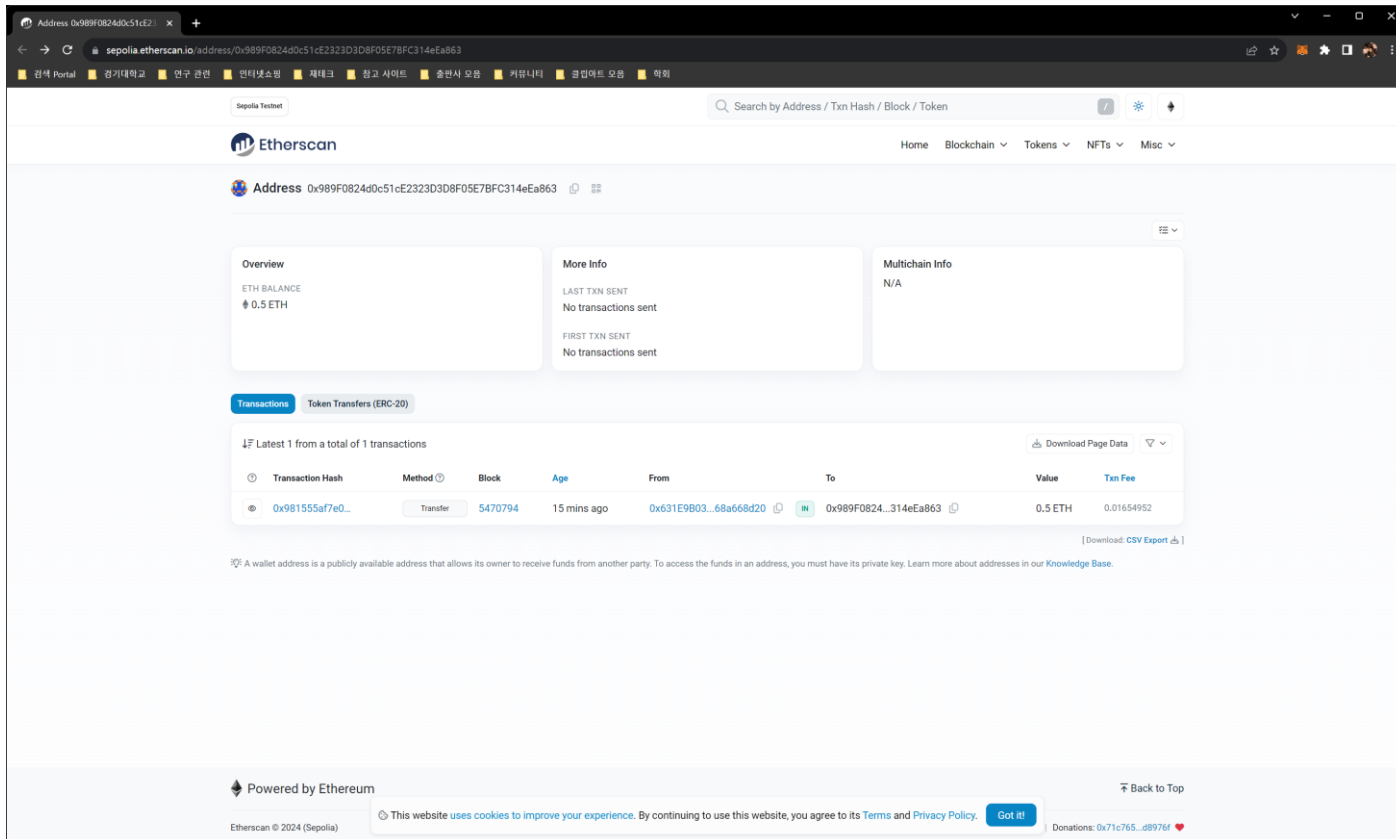
# 메타마스크 설치하기

- 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 for the address 0x989F0824d0c51cE2323D3D8F05E7BFC314eEa863. The page includes a search bar, navigation links (Home, Blockchain, Tokens, NFTs, Misc), and a detailed view of the address. The Overview section shows an ETH balance of 0.5 ETH. The More Info section shows no transactions sent. The Transactions section shows a single transaction (0x981555af7e0...) with a value of 0.5 ETH and a fee of 0.01654952. The page is powered by Ethereum and includes a cookie notice.

Address: 0x989F0824d0c51cE2323D3D8F05E7BFC314eEa863

Overview

ETH BALANCE  
0.5 ETH

More Info

LAST TXN SENT  
No transactions sent

FIRST TXN SENT  
No transactions sent

Multichain Info  
N/A

Transactions

Latest 1 from a total of 1 transactions

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x981555af7e0...	Transfer	5470794	15 mins ago	0x631E9B03...68a668d20	0x989F0824...314eEa863	0.5 ETH	0.01654952

Powered by Ethereum

This website uses cookies to improve your experience. By continuing to use this website, you agree to its Terms and Privacy Policy. Got it!

Back to Top

Etherscan © 2024 (Sepolia)

Donations: 0x71c765...d8976f ❤️



# 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 interface. The main content area displays transaction details for a specific hash. A red banner at the top of the details section states "[ This is a Sepolia Testnet transaction only ]". The transaction details are as follows:

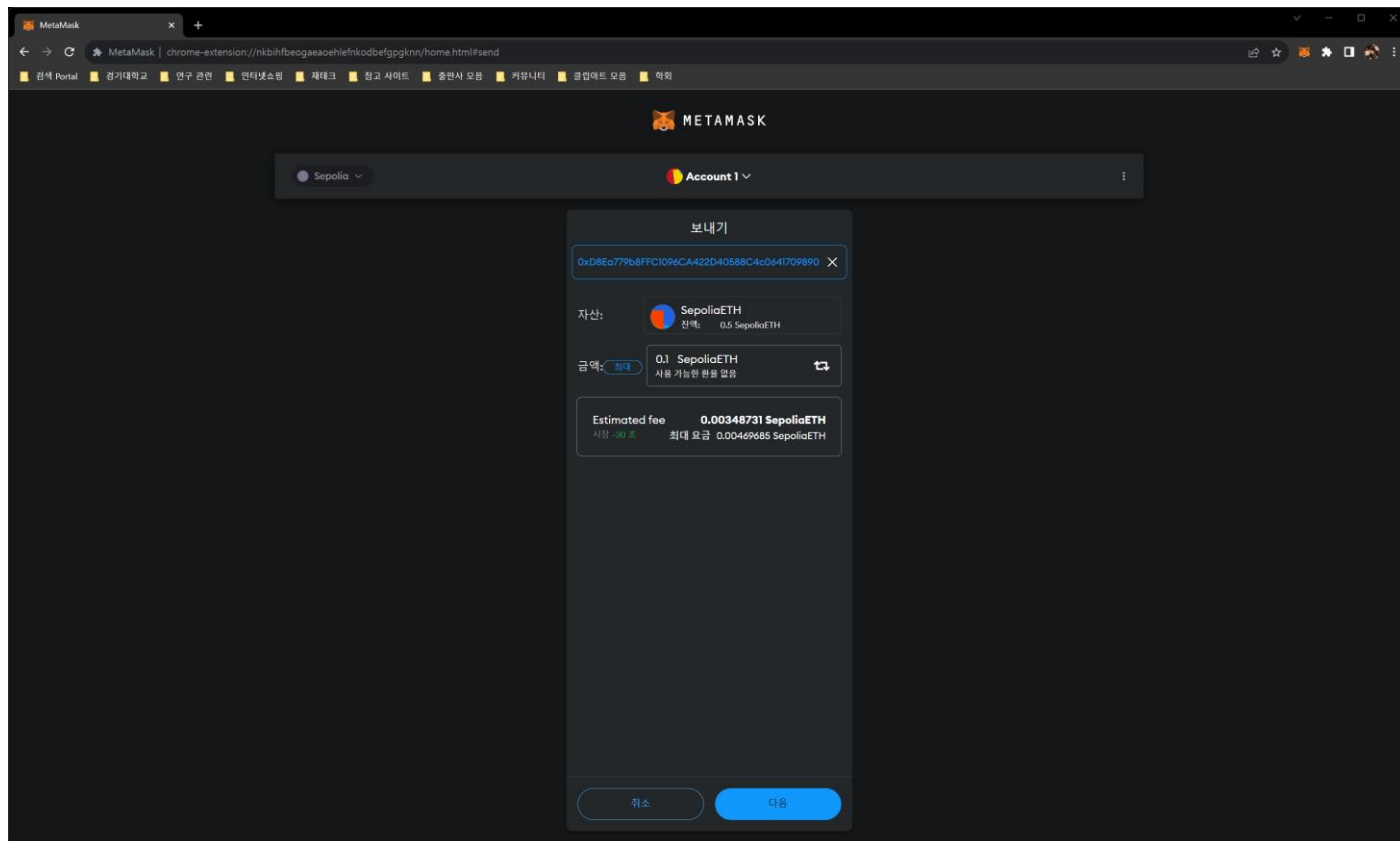
Field	Value
Transaction Hash:	0x981555af7e00dd21088e2f08ab7dcb399bd2e275dfd8c90d0790ebe848896d70
Status:	Success
Block:	5470794 (94 Block Confirmations)
Timestamp:	19 mins ago (Mar-12-2024 01:33:24 PM +UTC)
From:	0x631E9B031b16b18172a2B9D66C3668A68a668d20
To:	0x989F0824d0c51cE2323D3D8F05E78FC314eA863
Value:	0.5 ETH (\$0.00)
Transaction Fee:	0.016549523560668 ETH (\$0.00)
Gas Price:	788.072550508 Gwei (0.000000788072550508 ETH)

Below the details, there is a "More Details" section with a link to "Click to show more". At the bottom of the page, there is a footer with "Powered by Ethereum", a cookie consent banner, and a "Back to Top" link.



# 메타마스크 설치하기

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

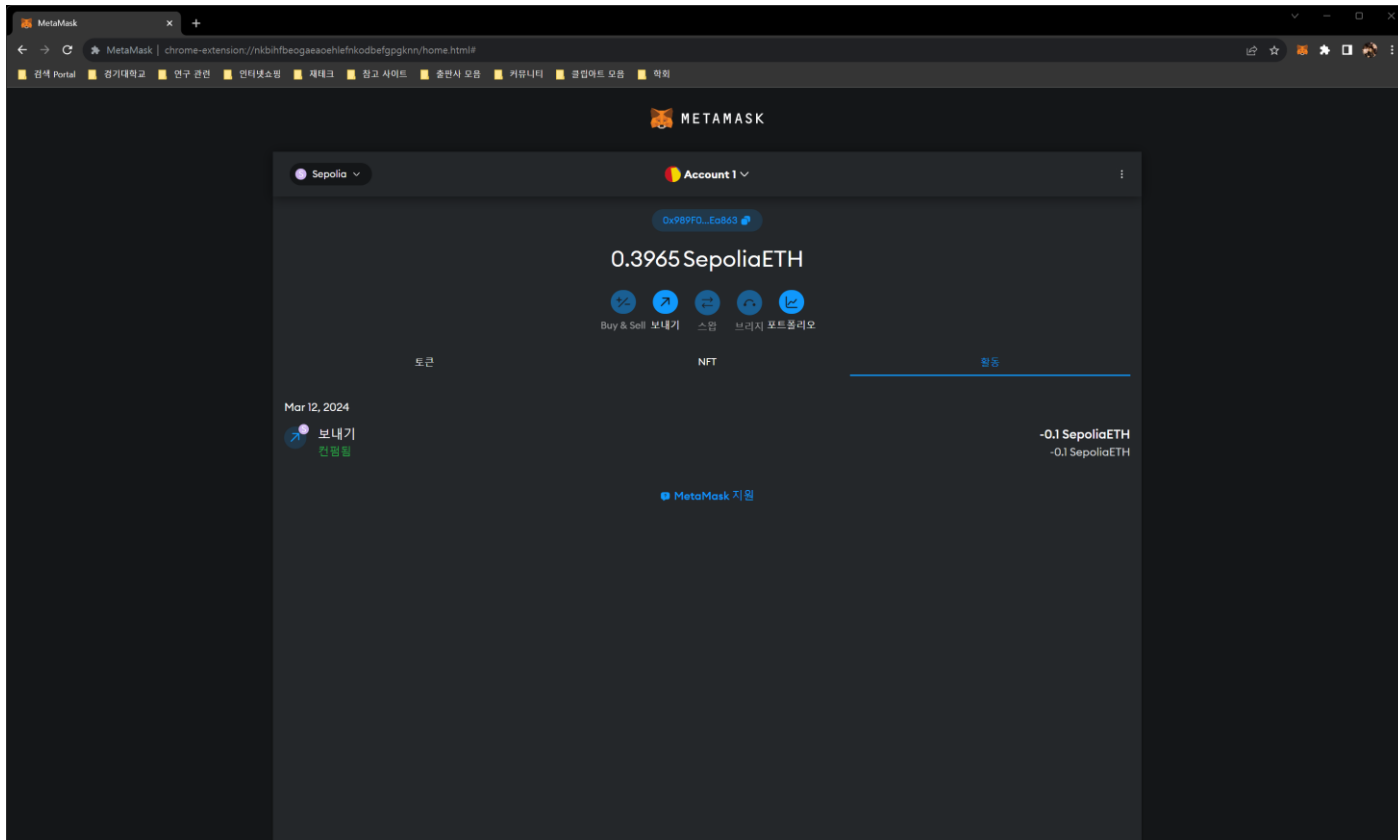






# 메타마스크 설치하기

- 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

```
pragma solidity 0.8.24;

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

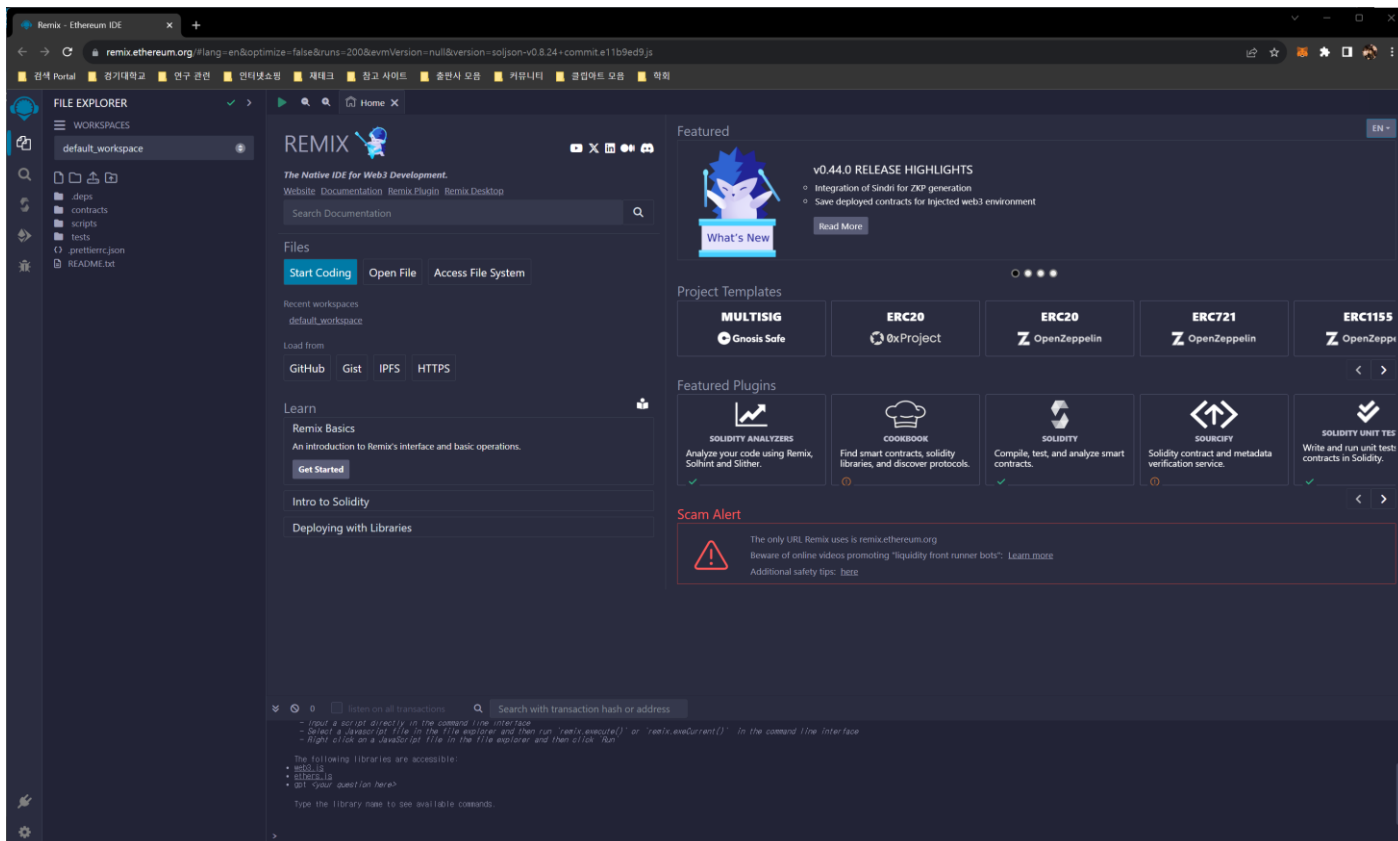
    // Give out ether to anyone who asks
    function withdraw(uint withdraw_amount) public {
        // Limit withdrawal amount
        require(withdraw_amount <= 1000000000000000000);

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



# Faucet 컨트랙트 컴파일

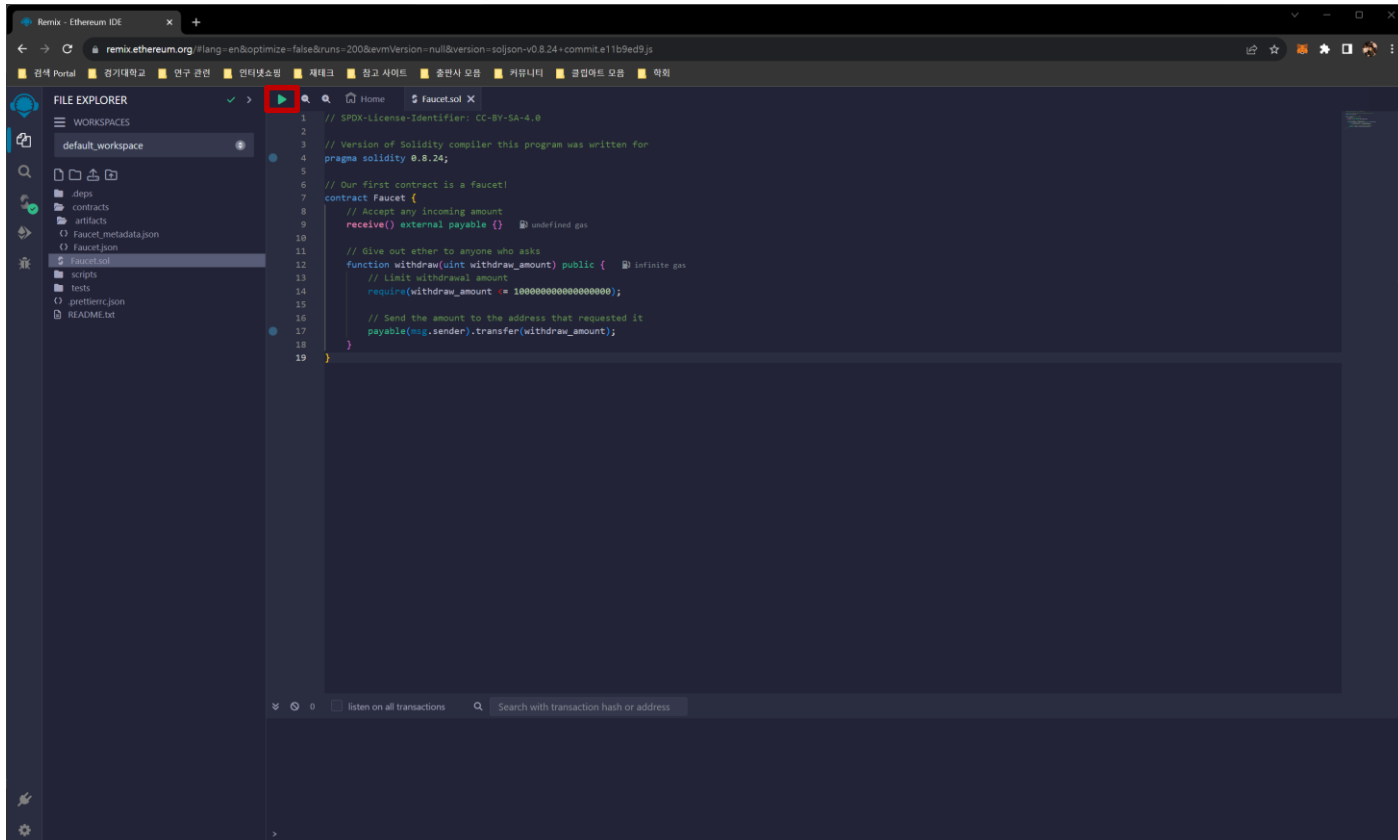
- 리믹스(Remix) IDE
  - 브라우저에서 솔리디티를 이용하여 스마트 컨트랙트를 개발하도록 도와주는 IDE
  - <https://remix.ethereum.org>





- 리믹스(Remix) IDE

- contracts 폴더 밑에 Faucet.sol 작성 후 컴파일







## Faucet 컨트랙트 컴파일

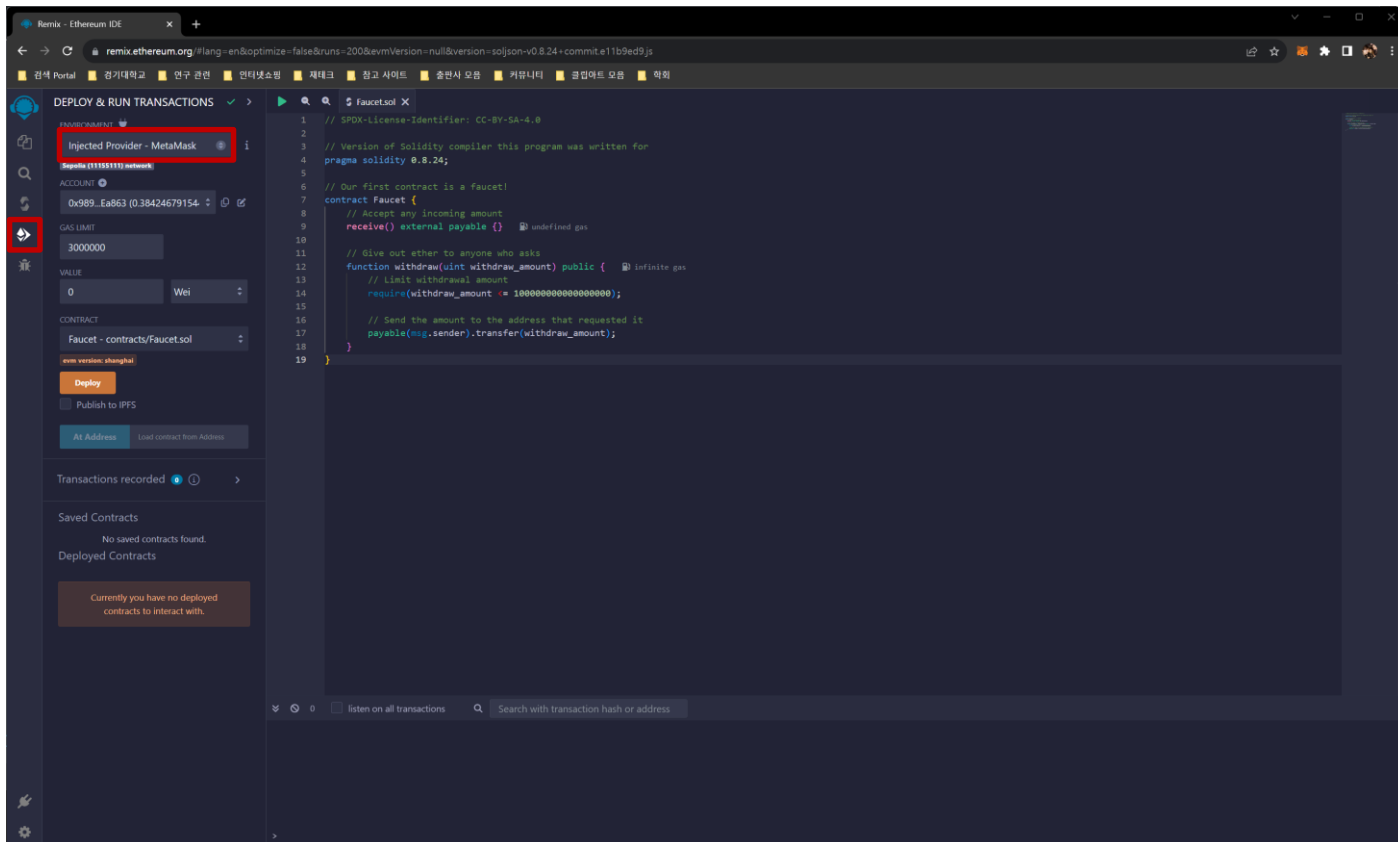
- 리믹스(Remix) IDE
  - 컴파일 결과 바이트 코드 (Faucet.json)

```
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
RETURNDATASIZE PUSH0 DUP1 RETURNDATACOPY RETURNDATASIZE 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

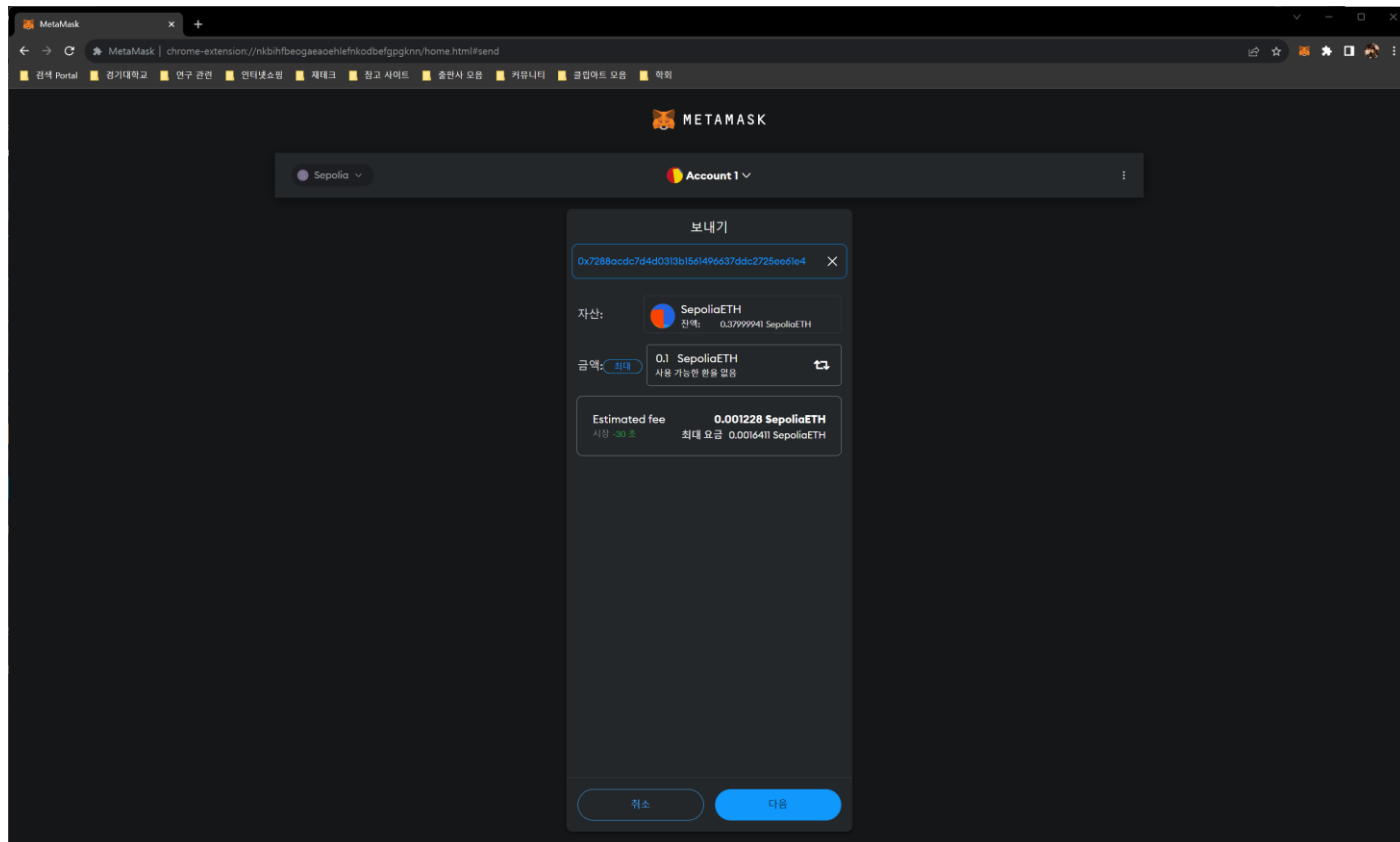
- 리믹스(Remix) IDE
  - Deploy & run transactions 탭
    - Deploy 결과

The screenshot shows the Etherscan Sepolia Testnet transaction details page. The transaction hash is 0x76622bce2ac878bf8d33ac0ca715baed3200d1562f609a7dbc5cefb0b58c937. The status is 'Success'. The block number is 5471537, with 43 block confirmations. The transaction occurred 9 minutes ago on March 12, 2024, at 04:06:12 PM UTC. The transaction action is a 'Call' to the method '0x80806040' by the address 0x989F0824...314Ea863. The transaction was sent from 0x989F0824d0c51cE2323D3D8F05E7BFC314Ea863 to 0x7288acdc7d4d0313b1561496637ddc2725ee61e4. The value is 0 ETH (\$0.00), the transaction fee is 0.004247384947051039 ETH (\$0.00), and the gas price is 34.281026861 Gwei (0.000000034281026861 ETH). A note at the bottom states: 'A transaction is a cryptographically signed instruction that changes the blockchain state. Block explorers track the details of all transactions in the network. Learn more about transactions in our Knowledge Base.'



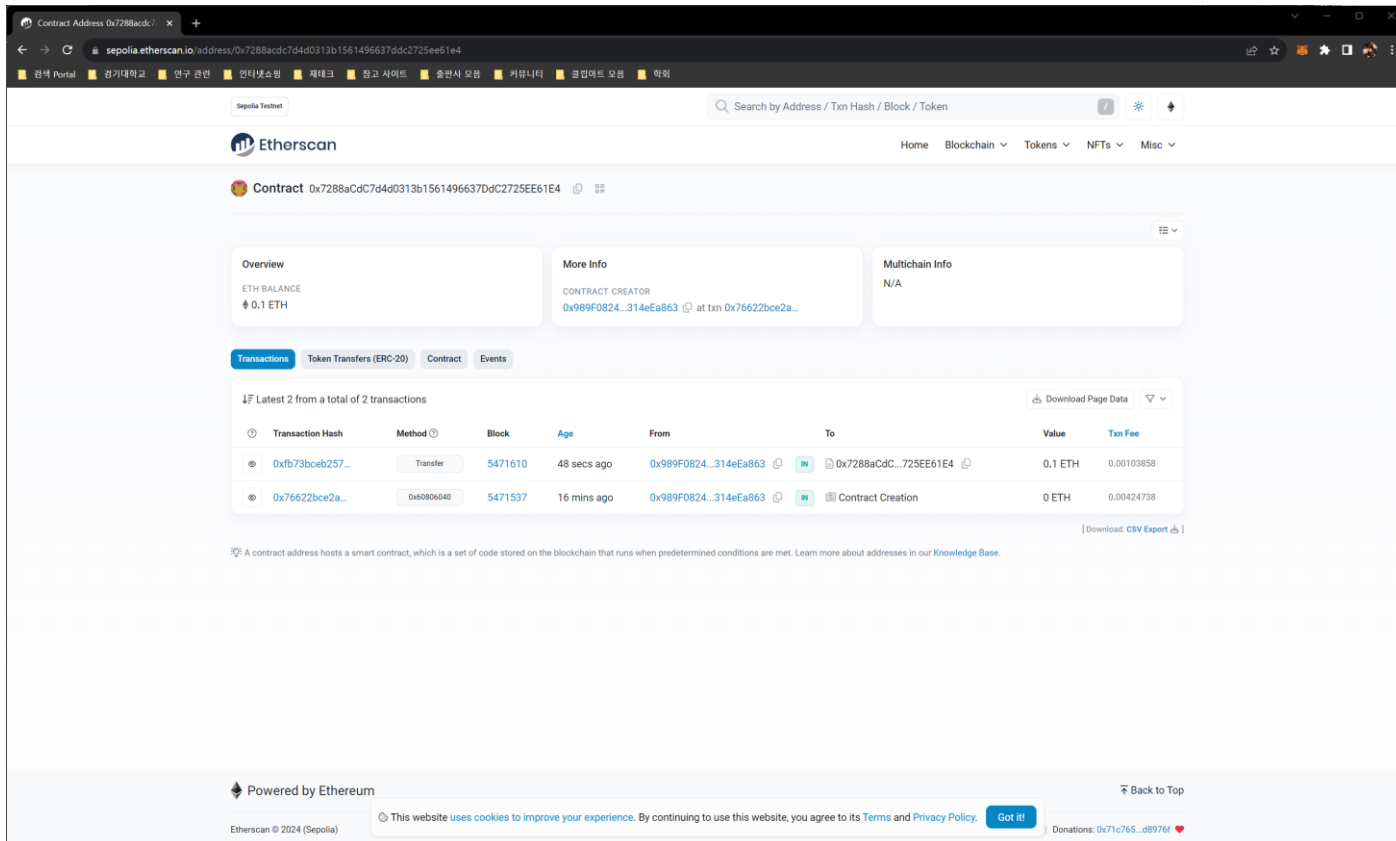
# 컨트랙트 사용하기

- 컨트랙트 자금 조달
  - 메타마스크를 통해 0.1 SepoliaETH 송금



# 컨트랙트 사용하기

- 컨트랙트 자금 조달
  - 송금 결과



The screenshot displays the Etherscan Sepolia Testnet interface for a specific contract address: `0x7288aCdC7d4d0313b1561496637DdC2725EE61E4`. The page is divided into several sections:

- Overview:** Shows the ETH balance as 0.1 ETH.
- More Info:** Lists the contract creator as `0x989F0824...314eEa863` at transaction `0x76622bce2a...`.
- Multichain Info:** Shows N/A.
- Transactions:** A table showing the latest 2 transactions from a total of 2.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
<a href="#">0xfb73bceb257...</a>	Transfer	5471610	48 secs ago	<a href="#">0x989F0824...314eEa863</a>	<a href="#">0x7288aCdC...725EE61E4</a>	0.1 ETH	0.00103858
<a href="#">0x76622bce2a...</a>	<code>0x60806040</code>	5471537	16 mins ago	<a href="#">0x989F0824...314eEa863</a>	Contract Creation	0 ETH	0.00424738

At the bottom, there is a footer with "Powered by Ethereum", a cookie consent banner, and a "Back to Top" link.



## 컨트랙트 사용하기

- 컨트랙트에서 출금



**THANK YOU!**