스마트 컨트랙트 활용 실습

목차

1. 실습 준비

1) 스마트 컨트랙트
2) 하이퍼렛저 베수 구동
3) Remix 활용
4) Web3 사용

2. 토큰 발행 실습

1) 토큰 발행 실습

3. 지갑 만들기

1) 지갑 만들기 실습

변수 / 데이터 타입

데이터 타입	키워드	사용	범위
Boolean	bool	True or False	True/ false
Uint	uint8	부호가 없는 정수 표현	0~255
	uint16		0~65535
	uint24		0~16777216
	uint256		0~
	uint		0~
String	string	문자열	-
Address	address	주소 잔액 조회	-
	address payable	주소 이더 전송	-
Array	DataType [ ]	배열 선언 • push: 가장 마지막 데이터 추가 • pop: 가장 마지막의 데이터를 가져오고 제거 • length: 배열의 길이 • struct: 구조체 선언	-
Map	Mapping (key type => value type)	맵	-

함수 및 옵션

```
function 함수 이름 () 옵션 {
    기능 정의
}
```

```
function tempFunction() view{

}

function tempFunction2() pure{

}
```

옵션

- view/pure를 사용하여 데이터 조회시 수수료를 지불하지 않음
- view는 변수값을 조회하여 반환 가능하나, pure는 변수에 접근 불가능
- view/pure가 붙은 함수는 데이터 변경이 불가능

View	Pure
• 상태 변수 값 변경 • 이벤트 발생 • 다른 계약 생성 • selfdestruct 사용 (해당 계약 계정을 삭제하고 모든 잔액을 지정된 주소로 이동) • 이더 전송 • view 혹은 pure로 선언되지 않은 어떠한 함수라도 호출 • 로우 레벨 호출 • 특정 OPCODE를 포함한 인라인 어셈블리 사용	• 상태 변수 읽기 • this.balance 혹은 <주소>.balance 접근 • Block, tx, msg중 하나의 맴버 변수에 접근 (msg.sig와 msg.data) 제외 • Pure로 정의되어 있지 않은 어떠한 함수라도 호출 • 특정 OPCODE를 포함한 인라인 어셈블리 사용

함수의 호출 범위 (가시성)

- Public: 모든 영역 (상속 받은 컨트랙트, 외부 컨트랙트, 내부)에서 함수 호출 가능
- Private: 해당 함수를 포함한 컨트랙트 내부에서만 호출 가능
- External: 다른 컨트랙트에서 호출하거나 트랜잭션으로만 호출 가능
- Internal: private와 비슷하지만 internal은 상속받은 컨트랙트에서도 호출 가능

```
function tempFunction() public view returns (uint256) {

}

function tempFunction2() private pure returns (string) {

}
```

스마트 컨트랙트

```
function tempFunction() public view returns (uint256) {

}

function tempFunction2() private pure returns (string) {

}
```

function 함수 이름 () 호출범위 옵션 return (return 데이터 타입) {
    기능 정의
}

생성자

```
1  pragma solidity >=0.4.22 <0.6.0;
2
3  contract mung{
4      uint vall;
5      address owner;
6      constructor(uint _v) public{
7          vall = _v;
8          owner = msg.sender;
9      }
```

- constructor 키워드를 사용
- 함수와 동일한 방법으로 사용
- 스마트 컨트랙트를 배포할 때 가장 처음 호출되는 함수
- Return 키워드 사용 불가

payable

```
1  pragma solidity >=0.4.22 <0.6.0;
2
3  contract mung{
4
5   function() external payable{
6       address sender = msg.sender;
7       uint value = msg.value;
8   }
9
10 }
11
```

- 외부로부터 이더를 받았을 때 호출하도록 하는 키워드
- Payable이 붙어 있으면 이더를 받았을때 호출하라는 의미가 있음
- payable이 붙은 경우 함수는 external이어야함
- msg.sender = 함수를 호출한 지갑 주소를 가져옴
- msg.value = 전송된 이더량

함수 변경자

```
1  pragma solidity >=0.4.22 <0.6.0;
2
3  contract mung{
4
5      address owner;
6
7      constructor() public {
8          owner = msg.sender;
9      }
10
11     modifier ownerCheck(){
12         require (msg.sender == owner);
13         _;
14     }
15
16     function getData() public view ownerCheck() returns (uint){
17         return 10;
18     }
19
20 }
```

- 함수변경자는 스마트 컨트랙트를 실행할 때 미리 실행되는 함수
- modifer 키워드 사용
- 예를들어 특정 지갑 주소만 함수를 호출할 수 있도록 설정 할때 사용

예외 처리

- require, assert를 이용

이벤트

- event 키워드를 사용
- 스마트 컨트랙트에서 특정한 일이 발생했을 때 외부에 알려주는 역할

address 타입의 자료형

- Address 타입의 자료형은 balance와 transfer 사용가능
- Balance는 특정 지갑 주소의 이더 보유량을 조회
- Transfer는 스마트 컨트랙트가 보유중인 이더를 다른 지갑 주소로 전송 가능

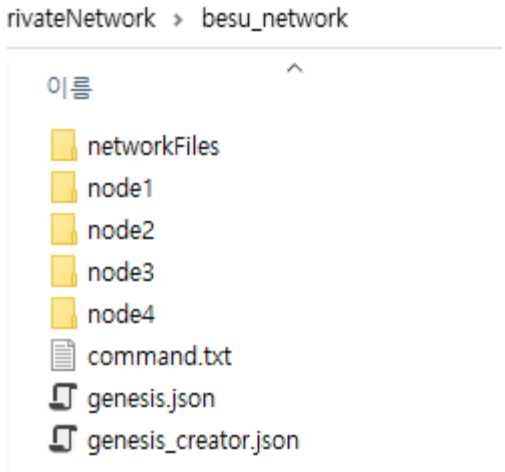
조건문, 반복문

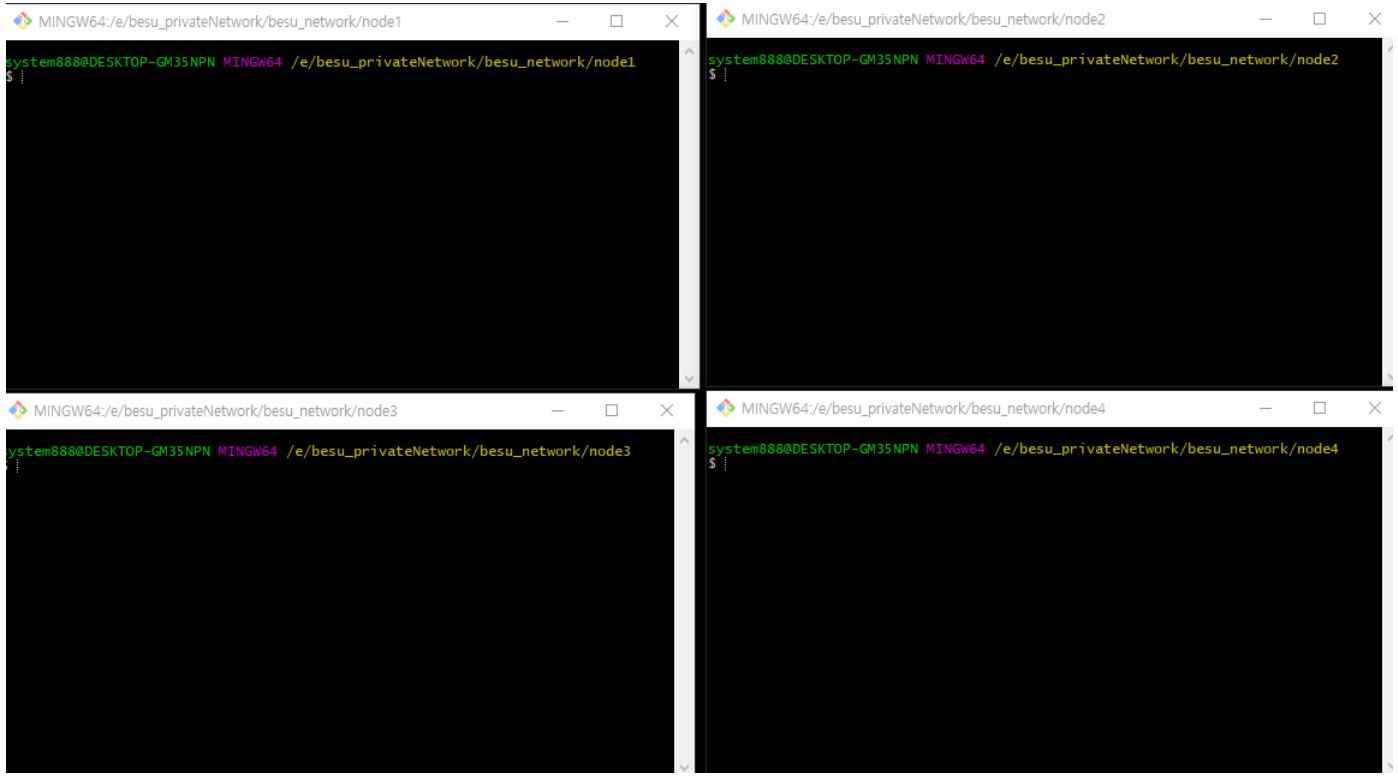
- 조건문 : if, if else, else
- 반복문: for

상속

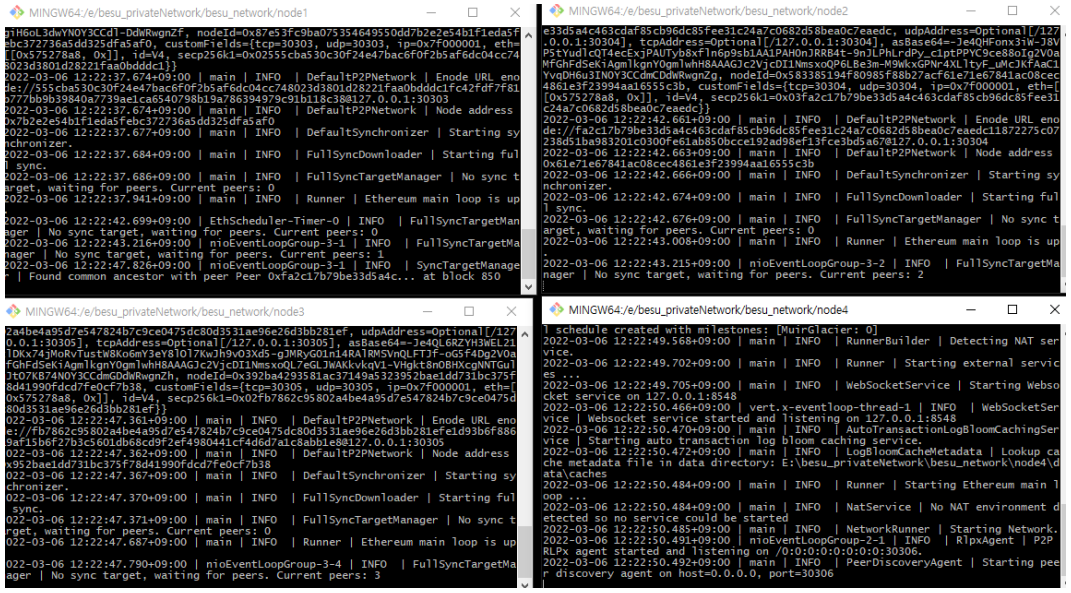
- is 키워드 사용
- public, internal 일때 사용 가능

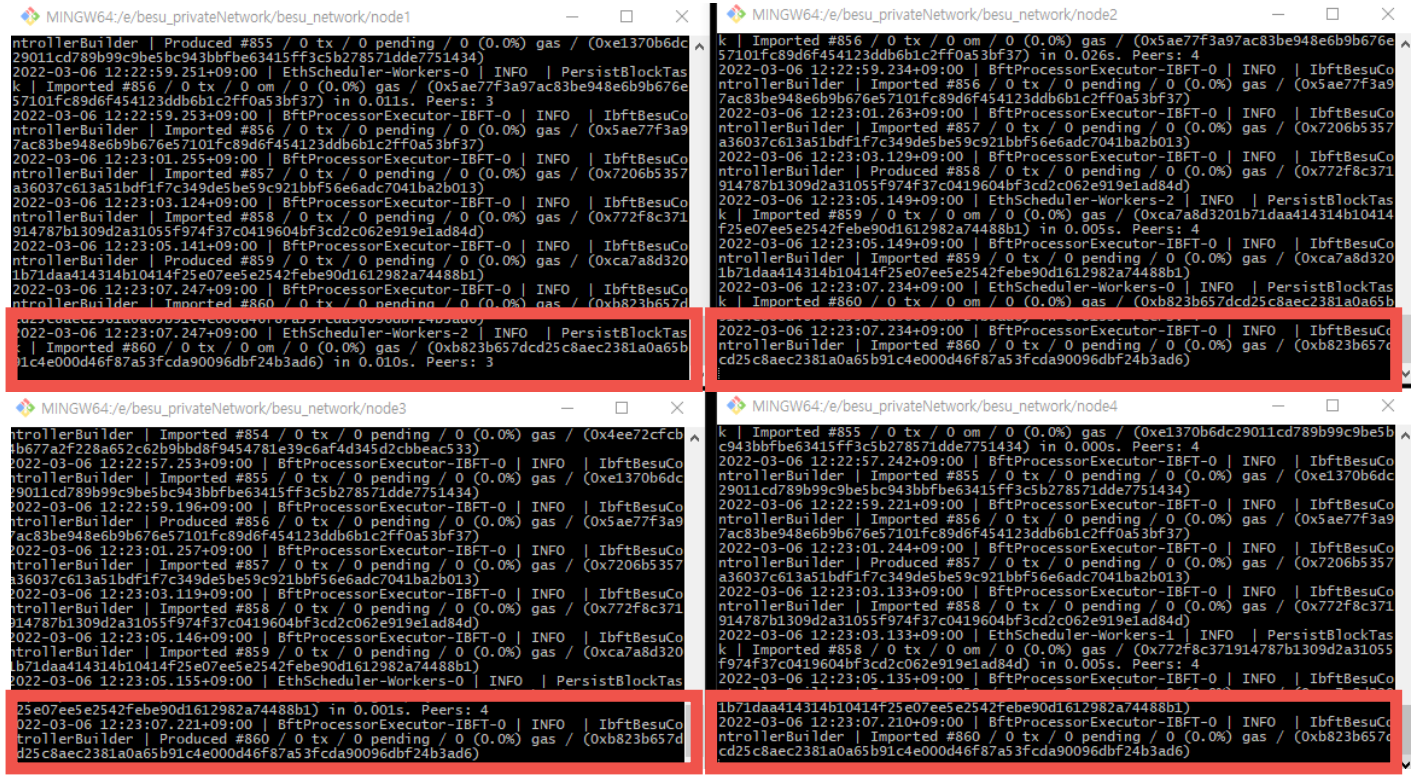
하이퍼렛저 베수 구동


rivateNetwork › besu_network
이름
networkFiles
node1
node2
node3
node4
command.txt
genesis.json
genesis_creator.json


MINGW64:/e/besu_privateNetwork/besu_network/node1
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_network/node1
$
MINGW64:/e/besu_privateNetwork/besu_network/node2
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_network/node2
$
MINGW64:/e/besu_privateNetwork/besu_network/node3
ystem888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_network/node3
MINGW64:/e/besu_privateNetwork/besu_network/node4
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_network/node4
$

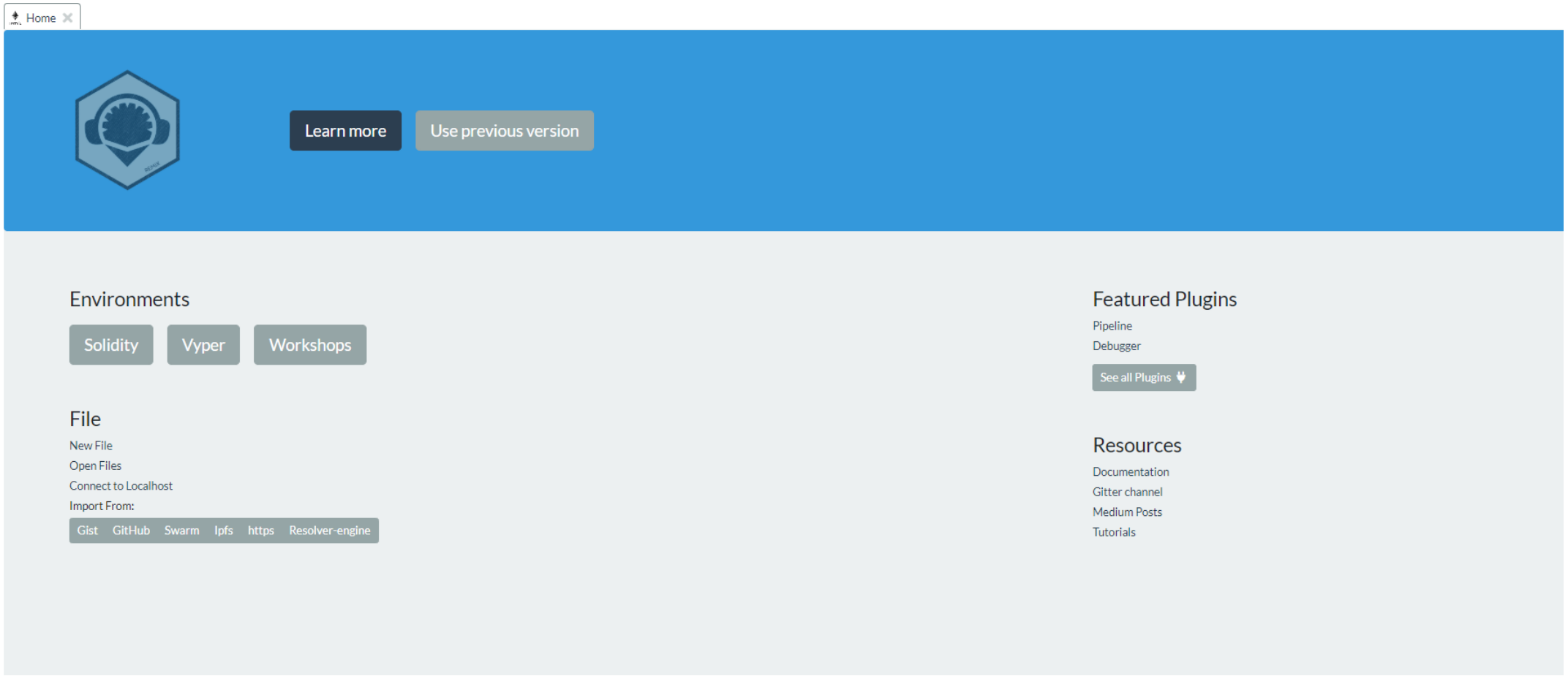
하이퍼렛저 베수 구동


MINGW64:/e/besu_privateNetwork/besu_network/node1
MINGW64:/e/besu_privateNetwork/besu_network/node2
MINGW64:/e/besu_privateNetwork/besu_network/node3
MINGW64:/e/besu_privateNetwork/besu_network/node4

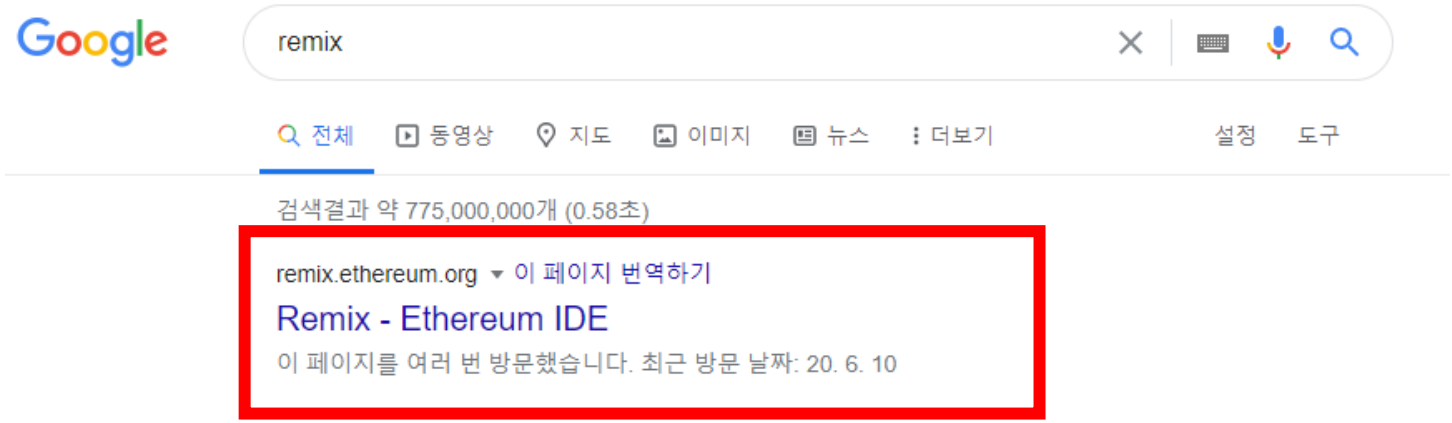

MINGW64:/e/besu_privateNetwork/besu_network/node1
MINGW64:/e/besu_privateNetwork/besu_network/node2
MINGW64:/e/besu_privateNetwork/besu_network/node3
MINGW64:/e/besu_privateNetwork/besu_network/node4

Remix 활용

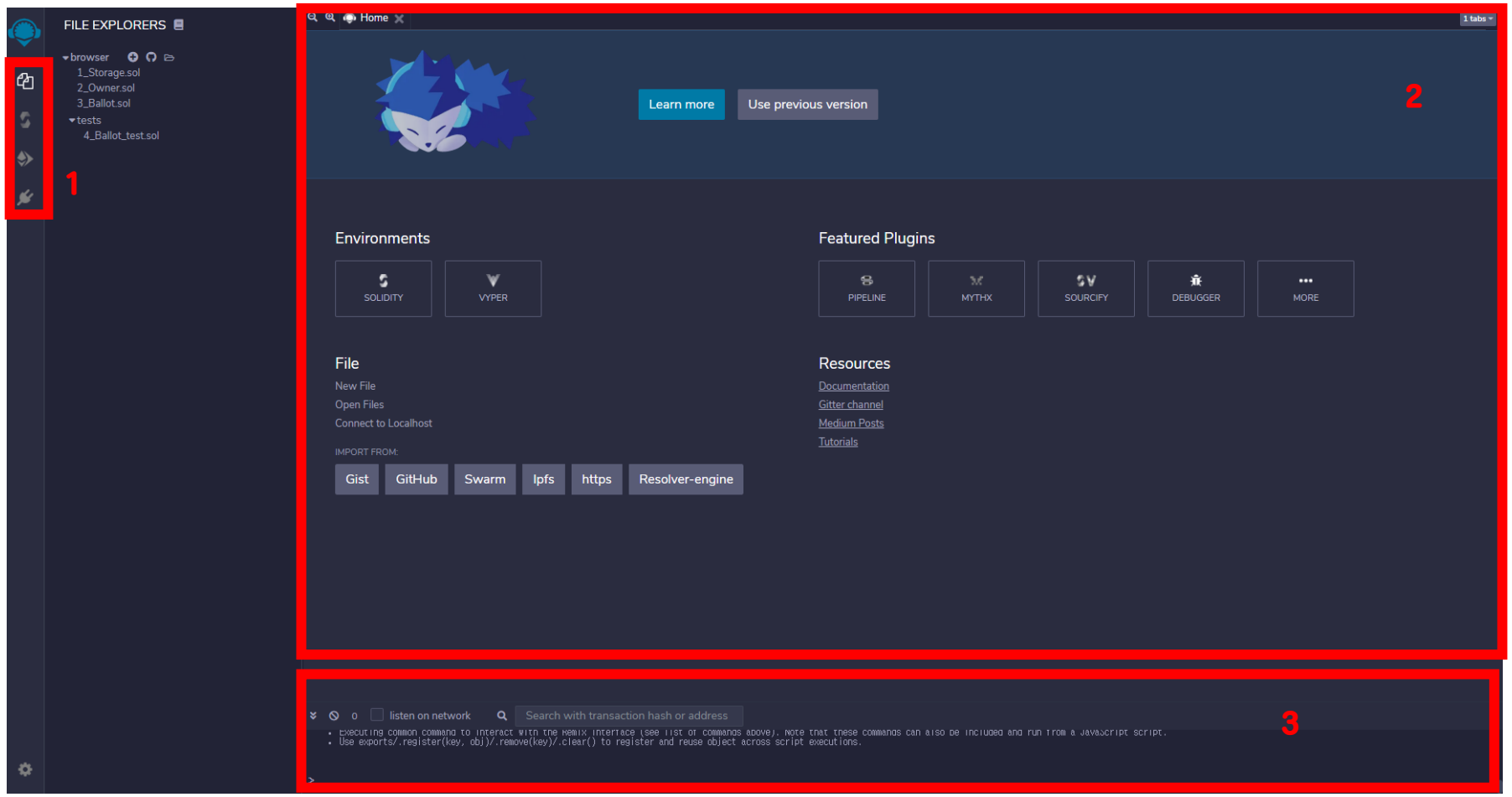
https://remix.ethereum.org/



Remix 활용


Google
remix
전체
동영상
지도
이미지
뉴스
더보기
설정
도구
검색결과 약 775,000,000개 (0.58초)
remix.ethereum.org
이 페이지 번역하기
Remix - Ethereum IDE
이 페이지를 여러 번 방문했습니다. 최근 방문 날짜: 20. 6. 10

Remix 활용

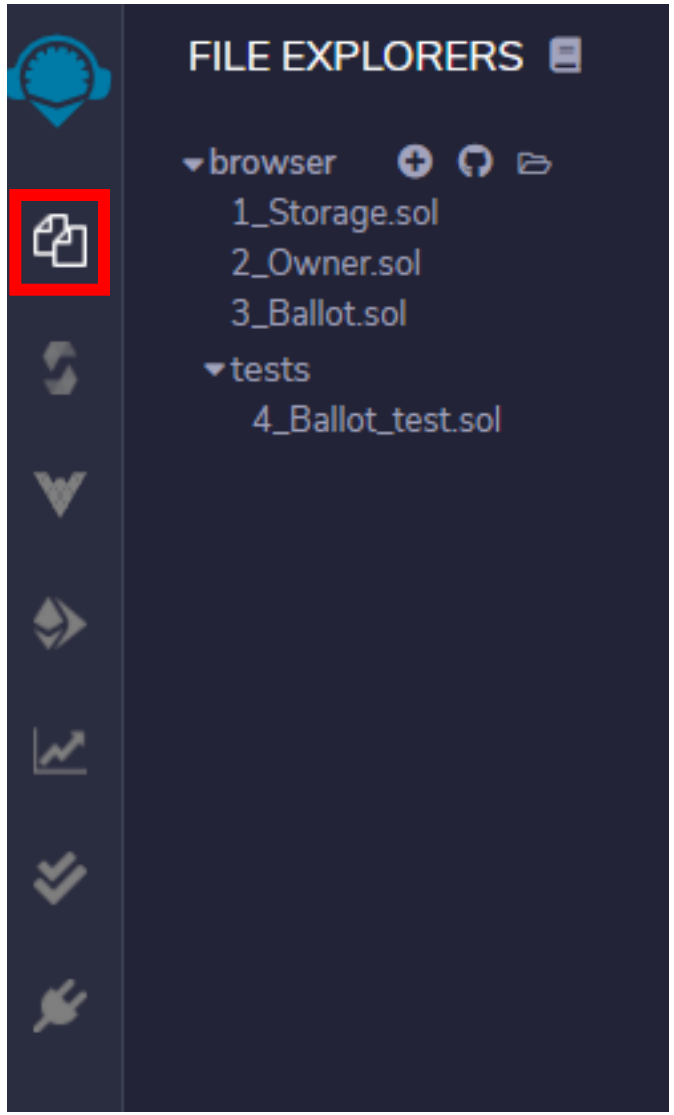


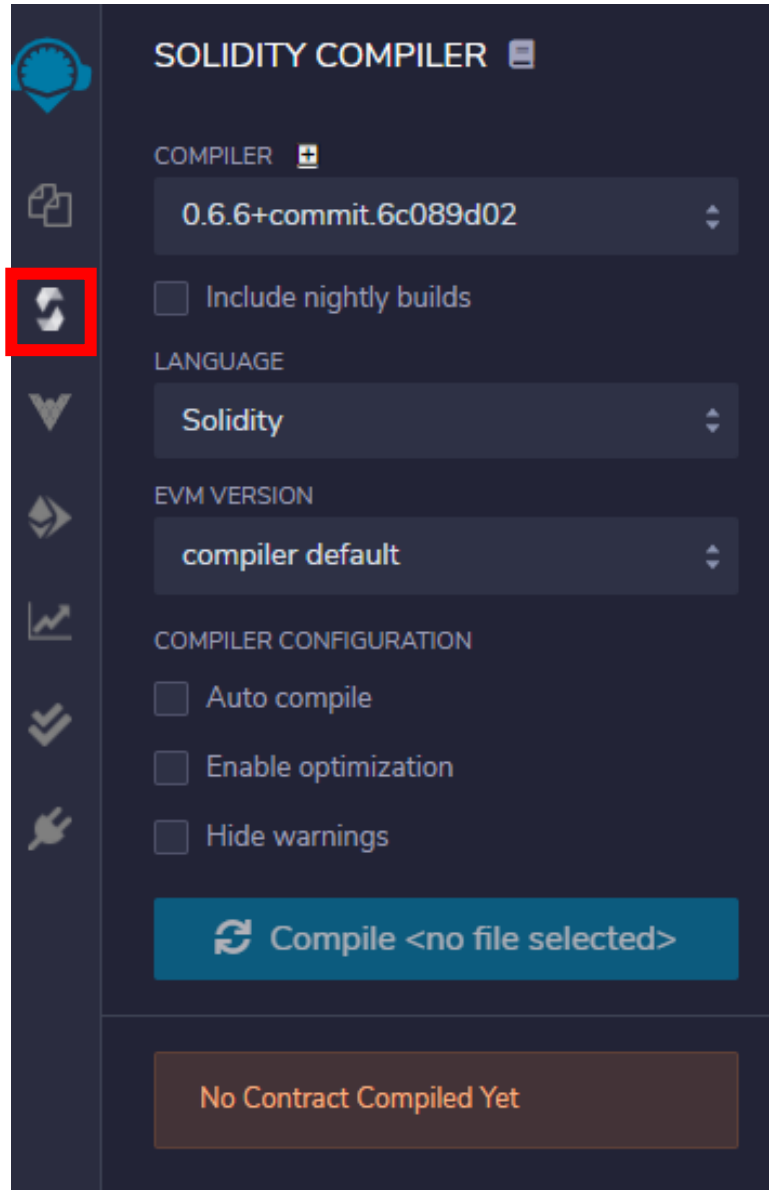
1. 탭

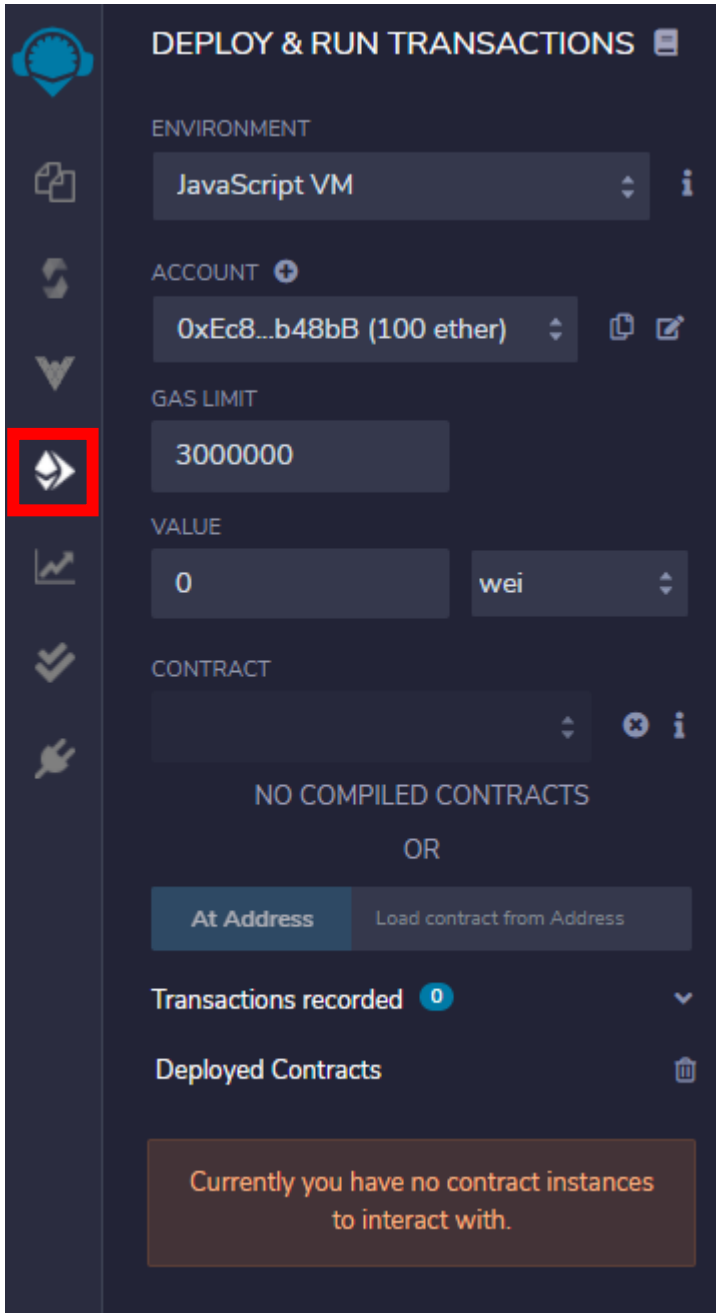
2. 메인 화면

3. 콘솔 화면

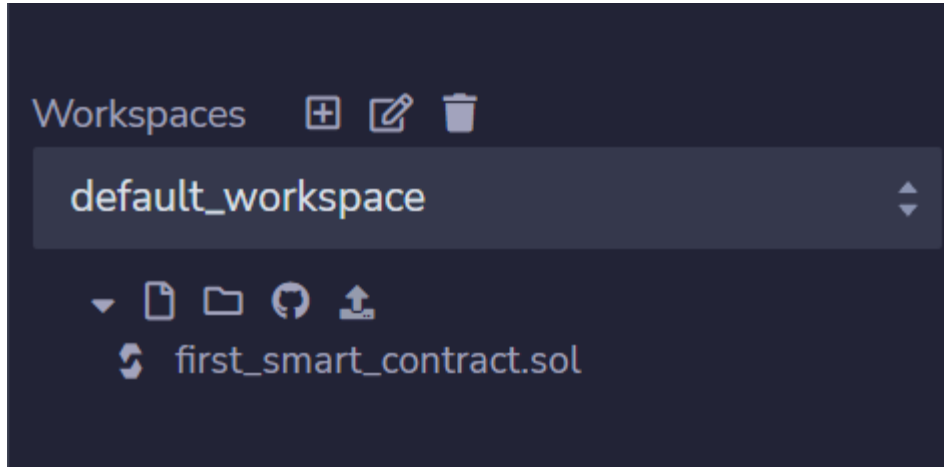
Remix 활용


FILE EXPLORERS
browser
1_Storage.sol
2_Owner.sol
3_Ballot.sol
tests
4_Ballot_test.sol


SOLIDITY COMPILER
COMPILER
0.6.6+commit.6c089d02
Include nightly builds
LANGUAGE
Solidity
EVM VERSION
compiler default
COMPILER CONFIGURATION
Auto compile
Enable optimization
Hide warnings
Compile <no file selected>
No Contract Compiled Yet

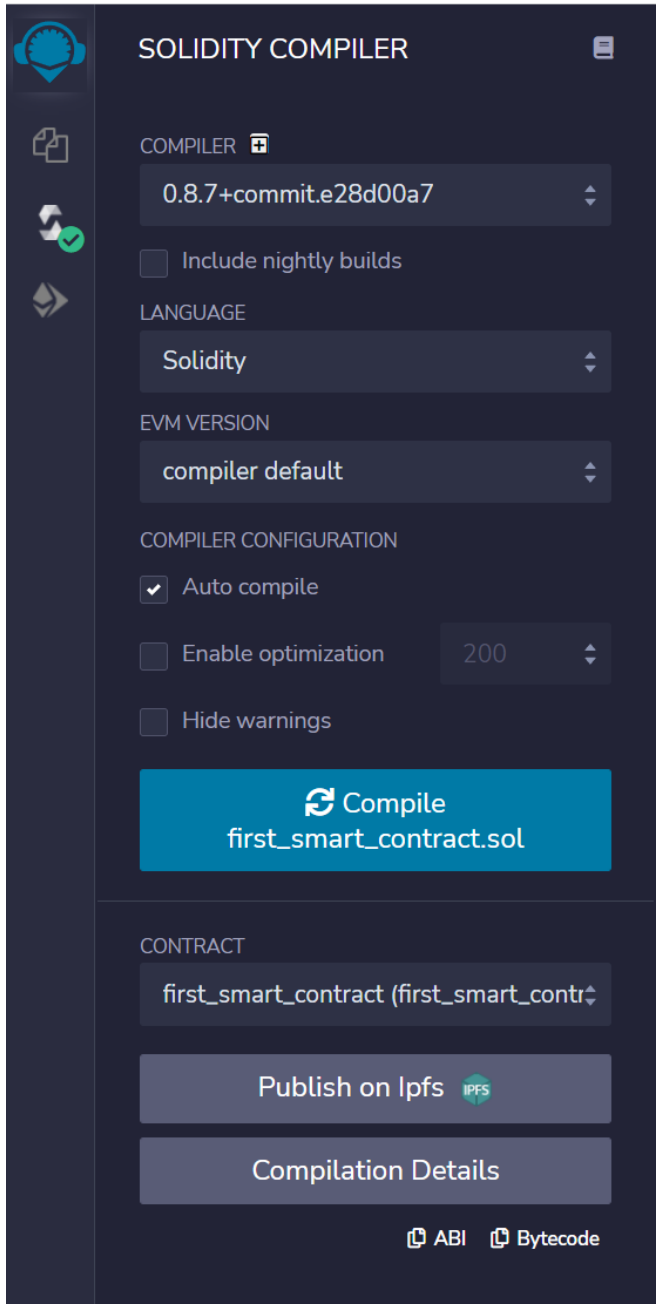

DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
JavaScript VM
ACCOUNT
0xEc8...b48bB (100 ether)
GAS LIMIT
3000000
VALUE
0
wei
CONTRACT
NO COMPILED CONTRACTS
OR
At Address
Load contract from Address
Transactions recorded 0
Deployed Contracts
Currently you have no contract instances to interact with.

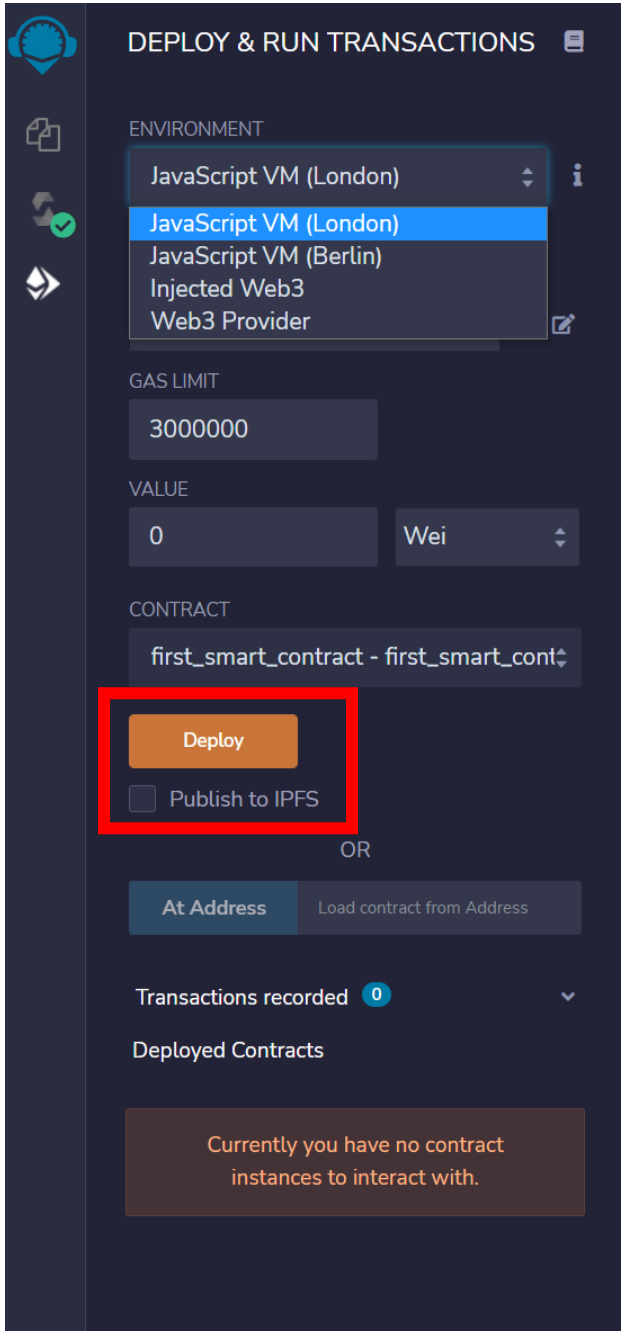
Remix 활용



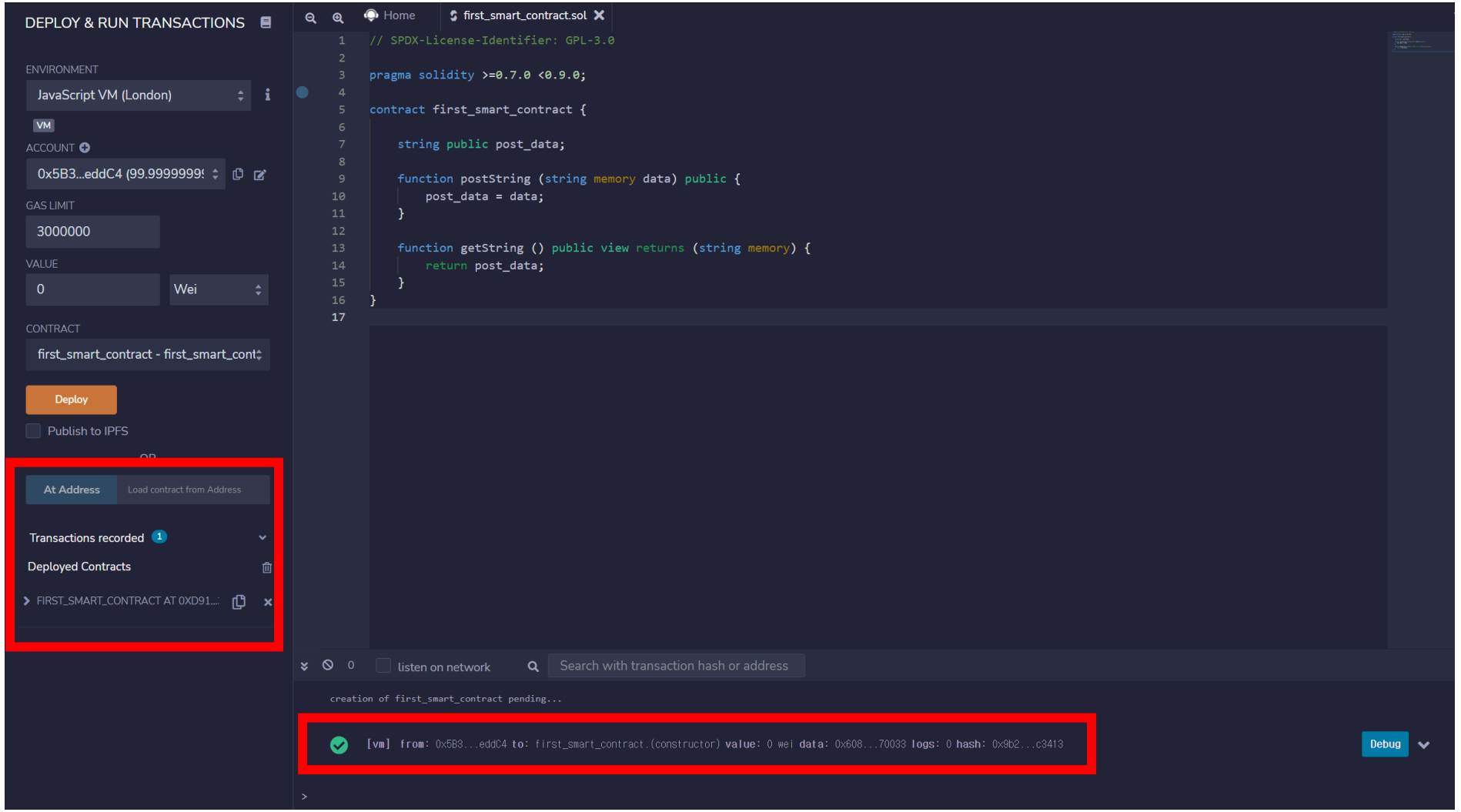

```sol
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.9.0;

contract first_smart_contract {

    string public post_data;

    function postString (string memory data) public {
        post_data = data;
    }

    function getString () public view returns (string memory) {
        return post_data;
    }
}
```

Remix 활용

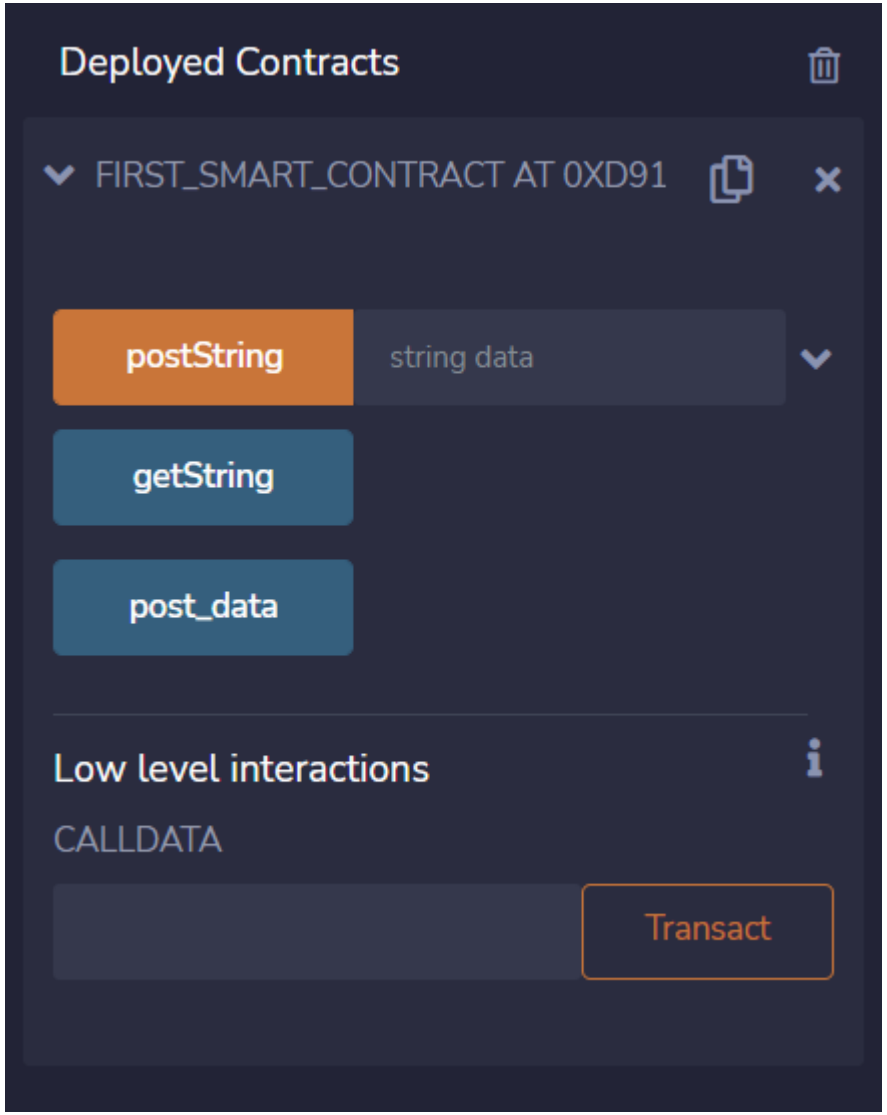

SOLIDITY COMPILER
COMPILER
0.8.7+commit.e28d00a7
Include nightly builds
LANGUAGE
Solidity
EVM VERSION
compiler default
COMPILER CONFIGURATION
Auto compile
Enable optimization
200
Hide warnings
Compile
first_smart_contract.sol
CONTRACT
first_smart_contract (first_smart_contr
Publish on Ipfs
Compilation Details
ABI
Bytecode


DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
JavaScript VM (London)
JavaScript VM (London)
JavaScript VM (Berlin)
Injected Web3
Web3 Provider
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
first_smart_contract - first_smart_cont
Deploy
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded
0
Deployed Contracts
Currently you have no contract instances to interact with.

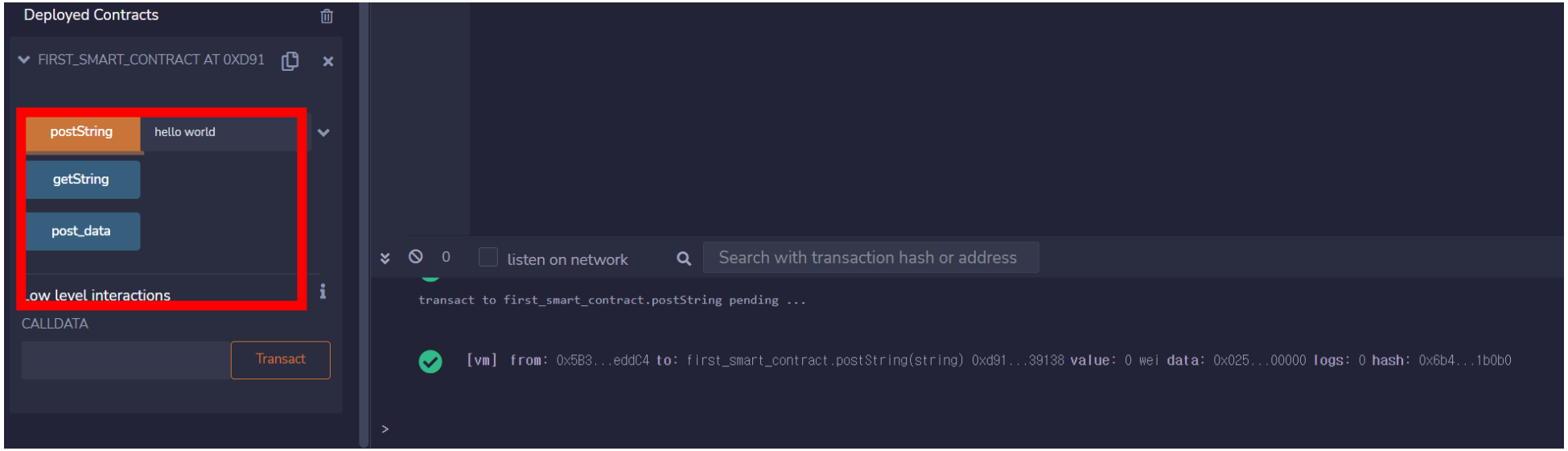
Remix 활용

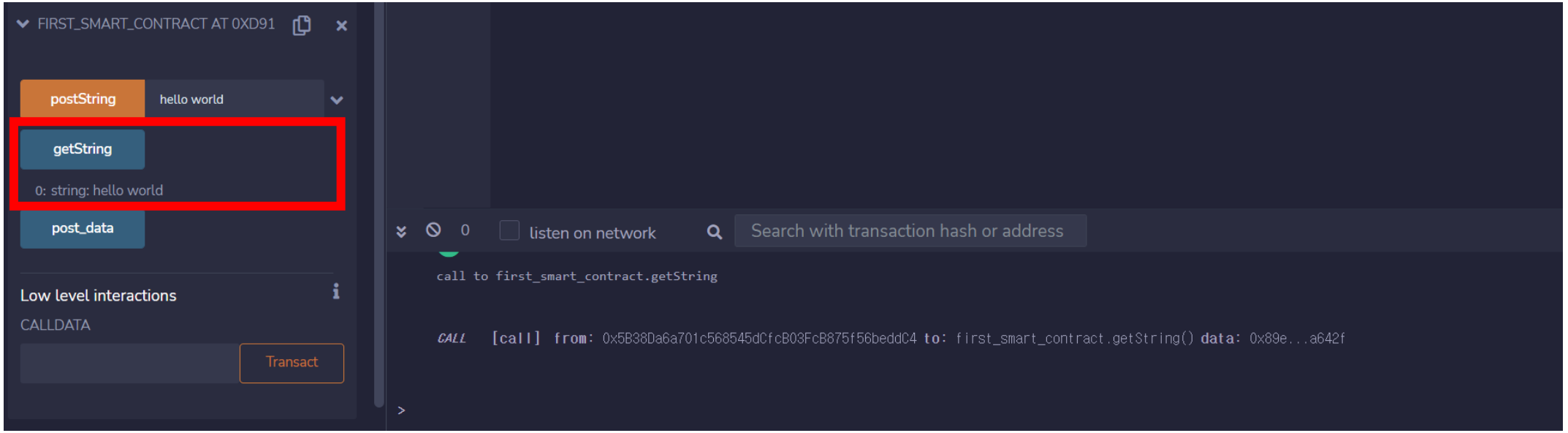

DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
JavaScript VM (London)
VM
ACCOUNT
0x5B3...eddC4 (99.9999999
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
first_smart_contract - first_smart_cont
Deploy
Publish to IPFS
At Address
Load contract from Address
Transactions recorded 1
Deployed Contracts
FIRST_SMART_CONTRACT AT 0XD91...
Home
first_smart_contract.sol
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.7.0 <0.9.0;
contract first_smart_contract {
string public post_data;
function postString (string memory data) public {
post_data = data;
}
function getString () public view returns (string memory) {
return post_data;
}
}
listen on network
Search with transaction hash or address
creation of first_smart_contract pending...
[vm] from: 0x5B3...eddC4 to: first_smart_contract.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x9b2...c3413
Debug

Remix 활용


Deployed Contracts
FIRST_SMART_CONTRACT AT 0XD91
postString
string data
getString
post_data
Low level interactions
CALLDATA
Transact

Remix 활용


Deployed Contracts
FIRST_SMART_CONTRACT AT 0XD91
postString
hello world
getString
post_data
Low level interactions
CALLDATA
Transact
0
listen on network
Search with transaction hash or address
transact to first_smart_contract.postString pending ...
[vm] from: 0x5B3...eddC4 to: first_smart_contract.postString(string) 0xd91...39138 value: 0 wei data: 0x025...00000 logs: 0 hash: 0x6b4...1b0b0
>


FIRST_SMART_CONTRACT AT 0XD91
postString
hello world
getString
0: string: hello world
post_data
Low level interactions
CALLDATA
Transact
0
listen on network
Search with transaction hash or address
call to first_smart_contract.getString
CALL [call] from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 to: first_smart_contract.getString() data: 0x89e...a642f
>

Node JS

목차

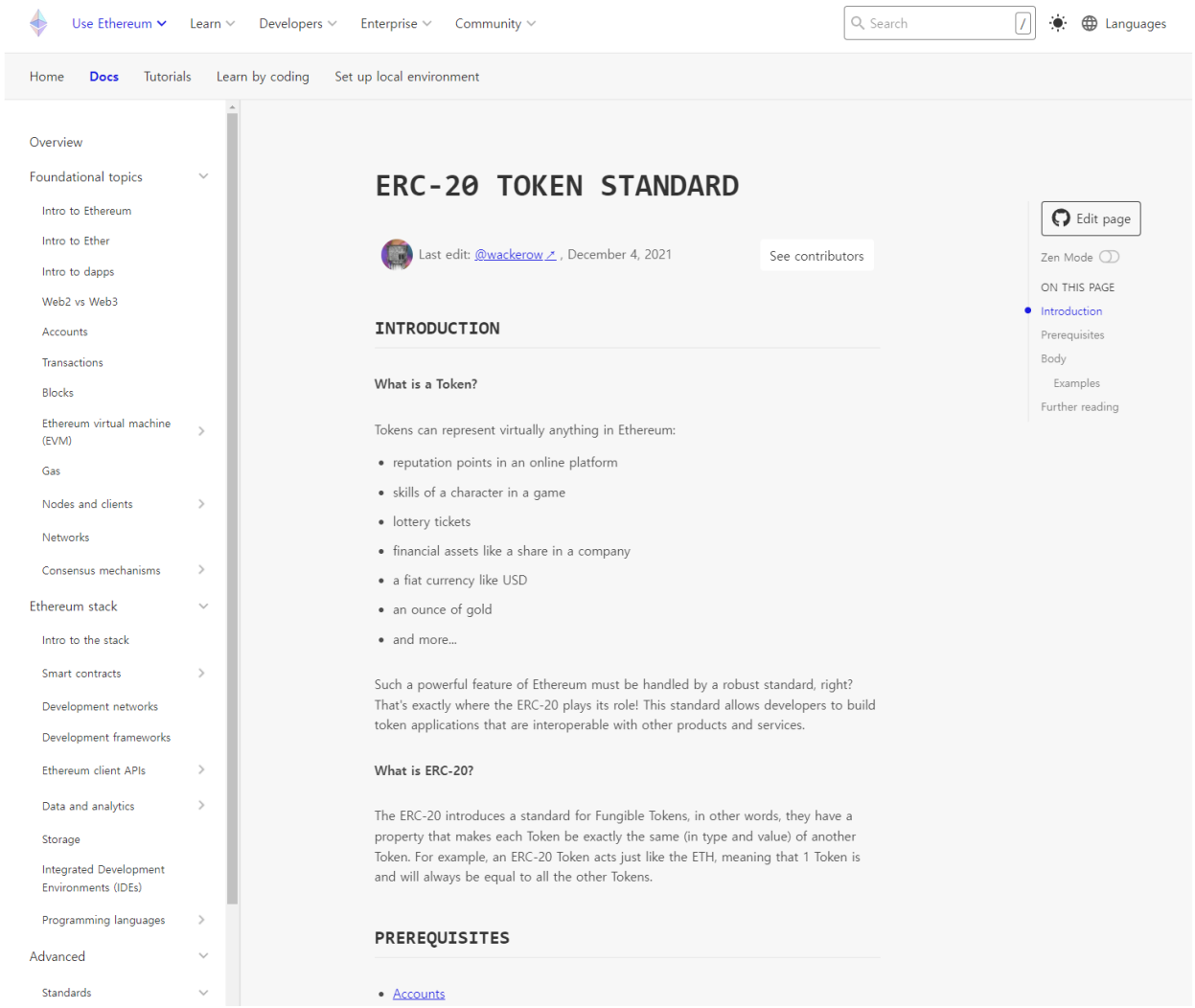
1. 실습 준비
   1) 스마트 컨트랙트
   2) 하이퍼렛저 베수 구동
   3) Remix 활용
   4) Web3 사용

2. 토큰 발행 실습
   1) 토큰 발행 실습

3. 지갑 만들기
   1) 지갑 만들기 실습

토큰 발행 실습

https://ethereum.org/en/developers/docs/standards/tokens/erc-20/



Methods

Show less | Copy

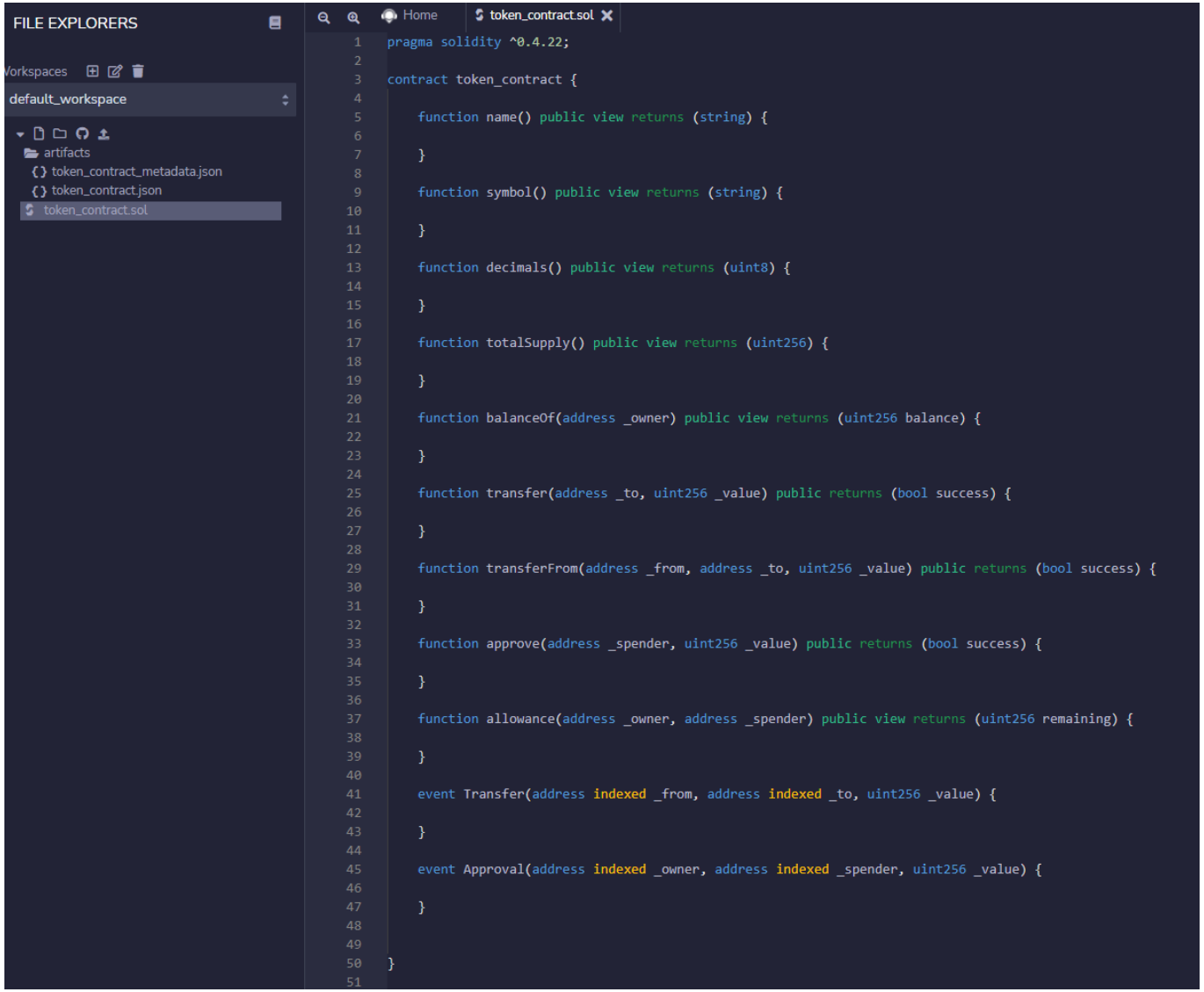
```
function name() public view returns (string)
function symbol() public view returns (string)
function decimals() public view returns (uint8)
function totalSupply() public view returns (uint256)
function balanceOf(address _owner) public view returns (uint256 balance)
function transfer(address _to, 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)

```

Events

Copy

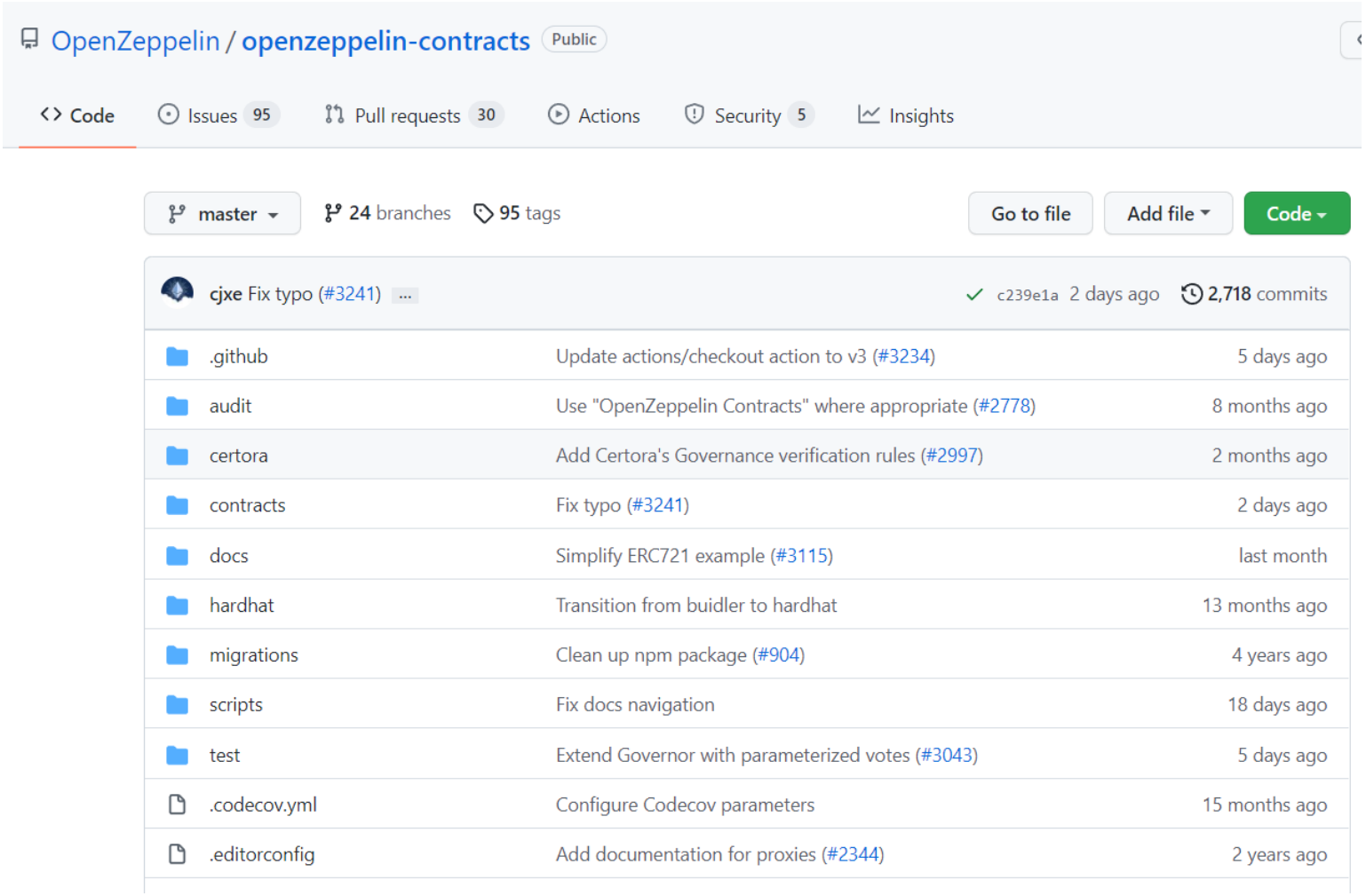
```
event Transfer(address indexed _from, address indexed _to, uint256 _value)
event Approval(address indexed _owner, address indexed _spender, uint256 _value)

```

토큰 발행 실습


FILE EXPLORERS
Workspaces
default_workspace
artifacts
token_contract_metadata.json
token_contract.json
token_contract.sol
Home
token_contract.sol
pragma solidity ^0.4.22;
contract token_contract {
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) {
}
event Transfer(address indexed _from, address indexed _to, uint256 _value) {
}
event Approval(address indexed _owner, address indexed _spender, uint256 _value) {
}
}

토큰 발행 실습

https://github.com/OpenZeppelin/openzeppelin-contracts



OpenZeppelin / openzeppelin-contracts Public

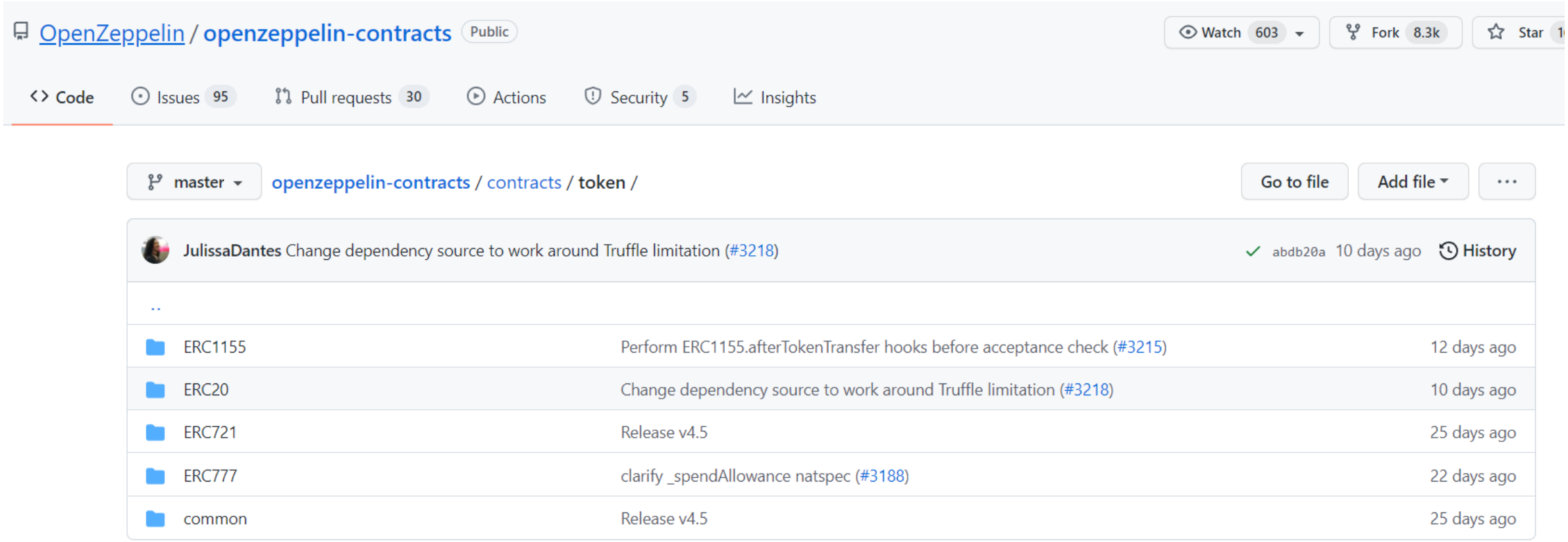
Code | Issues 95 | Pull requests 30 | Actions | Security 5 | Insights

master | 24 branches | 95 tags | Go to file | Add file | Code

cjxe Fix typo (#3241) ... c239e1a 2 days ago 2,718 commits

.github	Update actions/checkout action to v3 (#3234)	5 days ago
audit	Use "OpenZeppelin Contracts" where appropriate (#2778)	8 months ago
certora	Add Certora's Governance verification rules (#2997)	2 months ago
contracts	Fix typo (#3241)	2 days ago
docs	Simplify ERC721 example (#3115)	last month
hardhat	Transition from buidler to hardhat	13 months ago
migrations	Clean up npm package (#904)	4 years ago
scripts	Fix docs navigation	18 days ago
test	Extend Governor with parameterized votes (#3043)	5 days ago
.codecov.yml	Configure Codecov parameters	15 months ago
.editorconfig	Add documentation for proxies (#2344)	2 years ago

토큰 발행 실습


OpenZeppelin / openzeppelin-contracts
Public
Watch 603
Fork 8.3k
Star
Code
Issues 95
Pull requests 30
Actions
Security 5
Insights
master
openzeppelin-contracts / contracts / token /
Go to file
Add file
JulissaDantes Change dependency source to work around Truffle limitation (#3218)
abdb20a 10 days ago
History
..
ERC1155 Perform ERC1155.afterTokenTransfer hooks before acceptance check (#3215) 12 days ago
ERC20 Change dependency source to work around Truffle limitation (#3218) 10 days ago
ERC721 Release v4.5 25 days ago
ERC777 clarify _spendAllowance natspec (#3188) 22 days ago
common Release v4.5 25 days ago

토큰 발행 실습

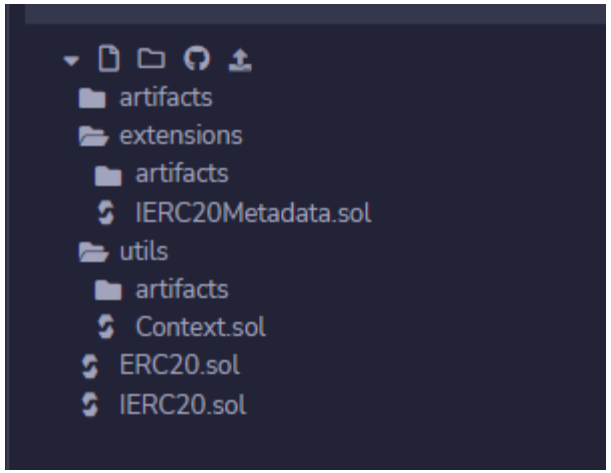
master openzeppelin-contracts / contracts / token / ERC20 / **ERC20.sol**

master openzeppelin-contracts / contracts / token / ERC20 / **IERC20.sol**

master openzeppelin-contracts / contracts / token / ERC20 / extensions / **IERC20Metadata.sol**

master openzeppelin-contracts / contracts / utils / **Context.sol**

토큰 발행 실습

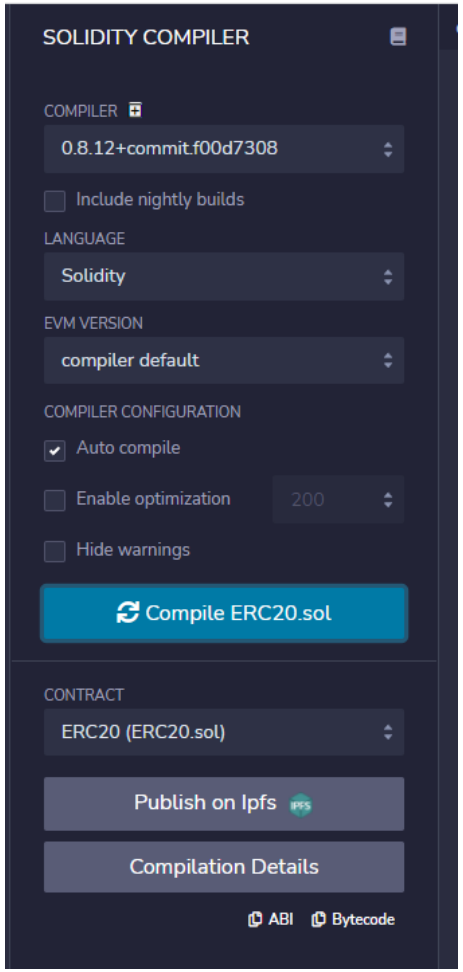


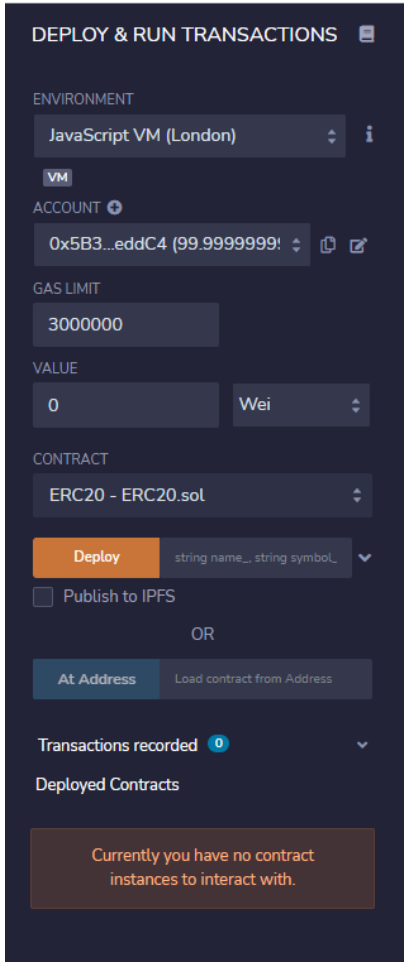
Home | ERC20.sol | IERC20Metadata.sol | IERC20.sol | Context.sol

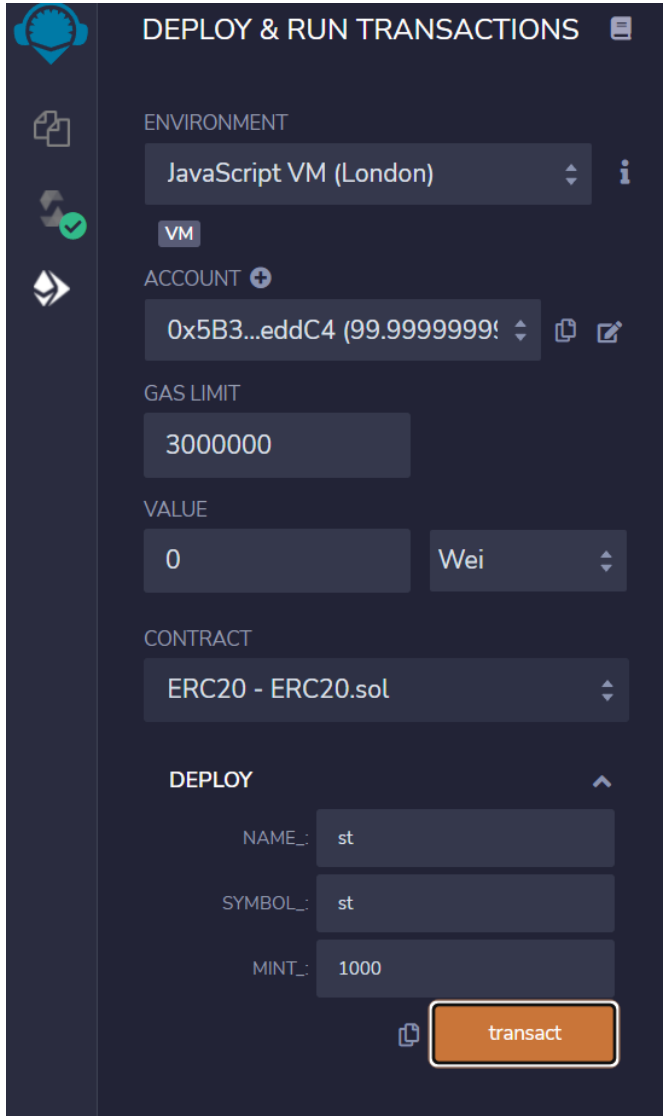
```
1  // SPDX-License-Identifier: MIT
2  // OpenZeppelin Contracts (last updated v4.5.0) (token/ERC20/ERC20.sol)
3
4  pragma solidity ^0.8.0;
5
6  import "./IERC20.sol";
7  import "./extensions/IERC20Metadata.sol";
8  import "./utils/Context.sol";
```

```
54     constructor(string memory name_, string memory symbol_, uint256 mint_) {
55         _name = name_;
56         _symbol = symbol_;
57         _mint(msg.sender, mint_);
58     }
```

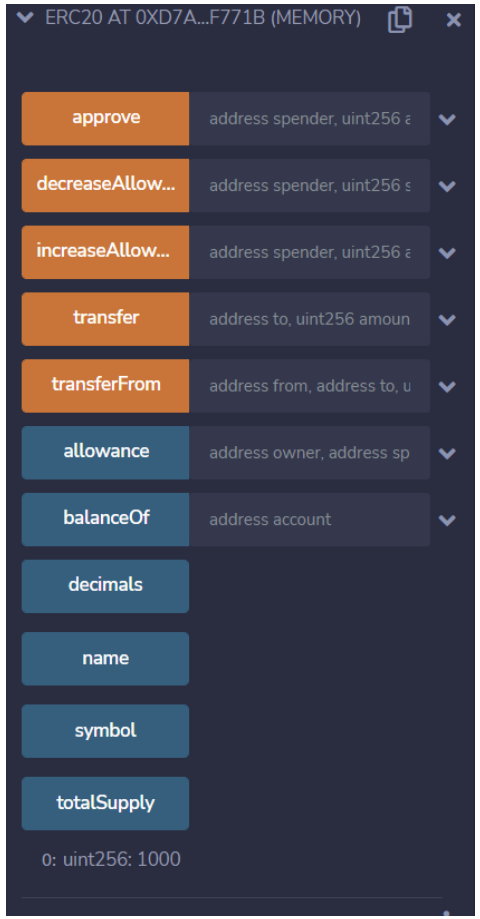
토큰 발행 실습

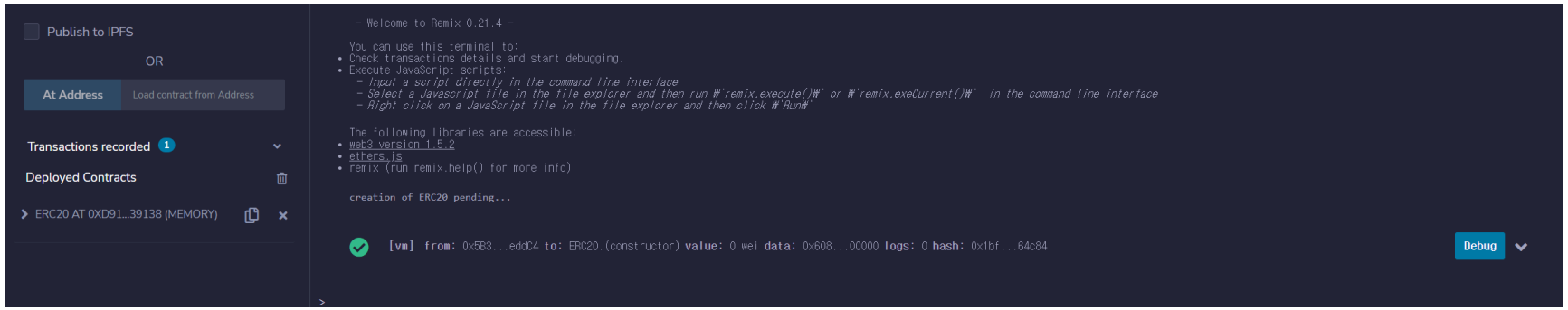

SOLIDITY COMPILER
COMPILER
0.8.12+commit.f00d7308
Include nightly builds
LANGUAGE
Solidity
EVM VERSION
compiler default
COMPILER CONFIGURATION
Auto compile
Enable optimization
200
Hide warnings
Compile ERC20.sol
CONTRACT
ERC20 (ERC20.sol)
Publish on Ipfs
Compilation Details
ABI
Bytecode


DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
JavaScript VM (London)
VM
ACCOUNT
0x5B3...eddC4 (99.9999999
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
ERC20 - ERC20.sol
Deploy
string name_, string symbol_
Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded
0
Deployed Contracts
Currently you have no contract instances to interact with.


DEPLOY & RUN TRANSACTIONS
ENVIRONMENT
JavaScript VM (London)
VM
ACCOUNT
0x5B3...eddC4 (99.9999999
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
ERC20 - ERC20.sol
DEPLOY
NAME_:
st
SYMBOL_:
st
MINT_:
1000
transact

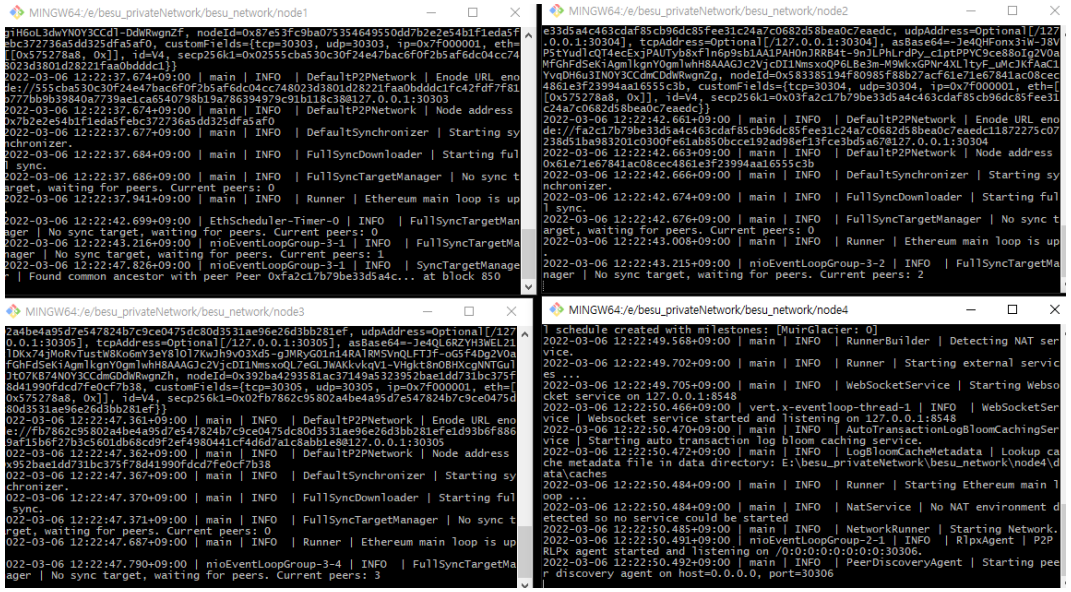
토큰 발행 실습

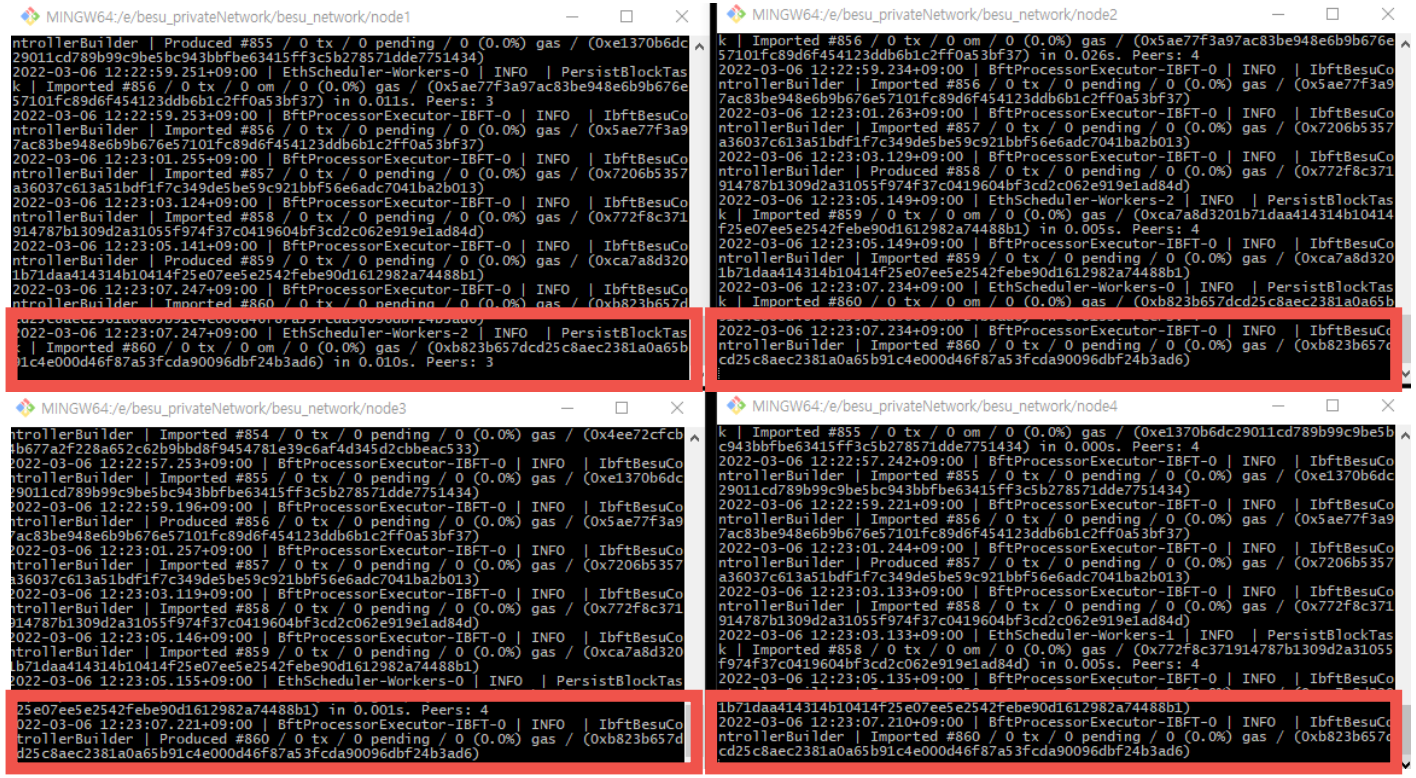

ERC20 AT 0XD7A...F771B (MEMORY)
approve
address spender, uint256 a
decreaseAllow...
address spender, uint256 s
increaseAllow...
address spender, uint256 a
transfer
address to, uint256 amoun
transferFrom
address from, address to, u
allowance
address owner, address sp
balanceOf
address account
decimals
name
symbol
totalSupply
0: uint256: 1000


Publish to IPFS
OR
At Address
Load contract from Address
Transactions recorded 1
Deployed Contracts
ERC20 AT 0XD91...39138 (MEMORY)
- Welcome to Remix 0.21.4 -
You can use this terminal to:
• Check transactions details and start debugging.
• Execute JavaScript scripts:
- Input a script directly in the command line interface
- Select a Javascript file in the file explorer and then run #'remix.execute()#' or #'remix.exeCurrent()#' in the command line interface
- Right click on a JavaScript file in the file explorer and then click #'Run#'
The following libraries are accessible:
• web3 version 1.5.2
• ethers.js
• remix (run remix.help() for more info)
creation of ERC20 pending...
[vm] from: 0x5B3...eddC4 to: ERC20.(constructor) value: 0 wei data: 0x608...00000 logs: 0 hash: 0x1bf...64c84
Debug

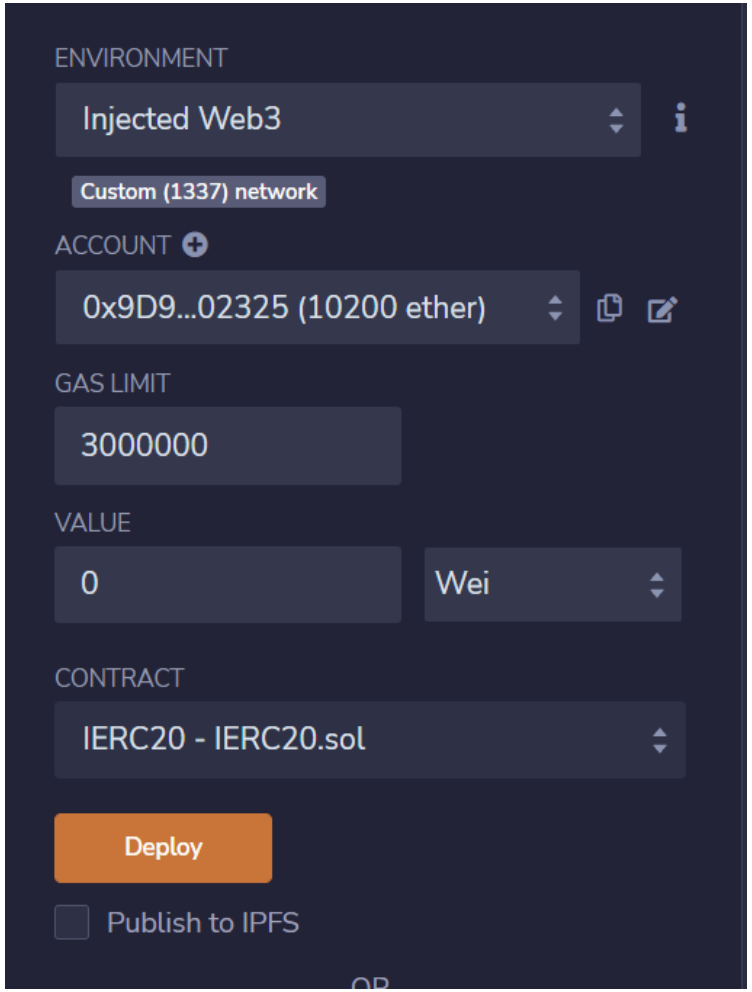
토큰 발행 실습

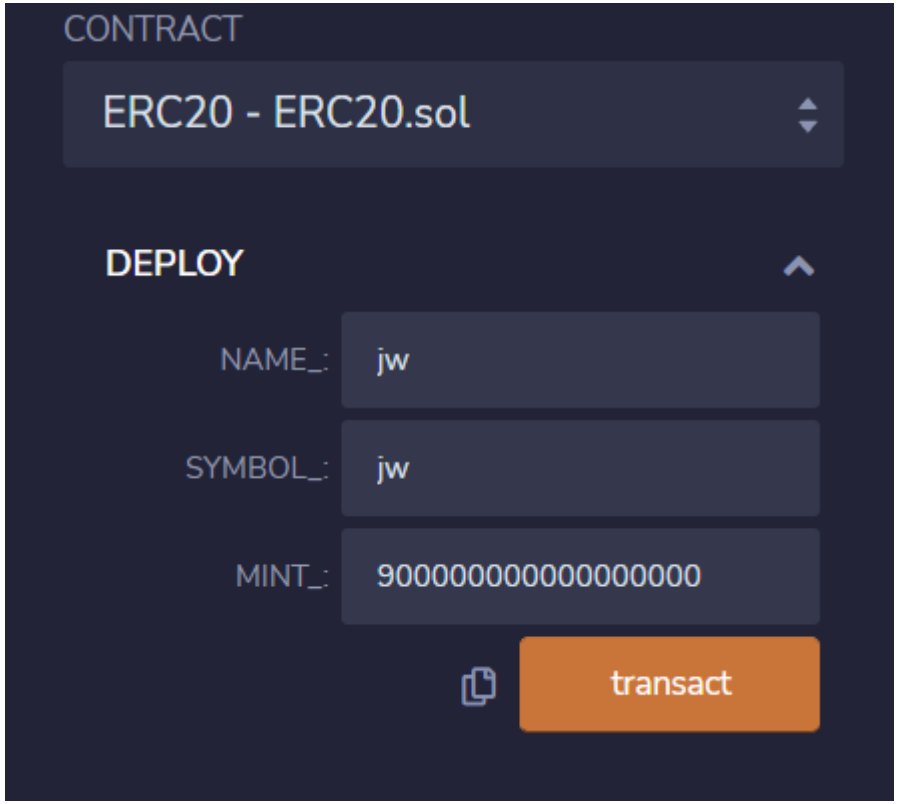
베수 실행


MINGW64:/e/besu_privateNetwork/besu_network/node1
MINGW64:/e/besu_privateNetwork/besu_network/node2
MINGW64:/e/besu_privateNetwork/besu_network/node3
MINGW64:/e/besu_privateNetwork/besu_network/node4


MINGW64:/e/besu_privateNetwork/besu_network/node1
MINGW64:/e/besu_privateNetwork/besu_network/node2
MINGW64:/e/besu_privateNetwork/besu_network/node3
MINGW64:/e/besu_privateNetwork/besu_network/node4

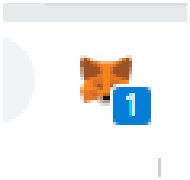
토큰 발행 실습

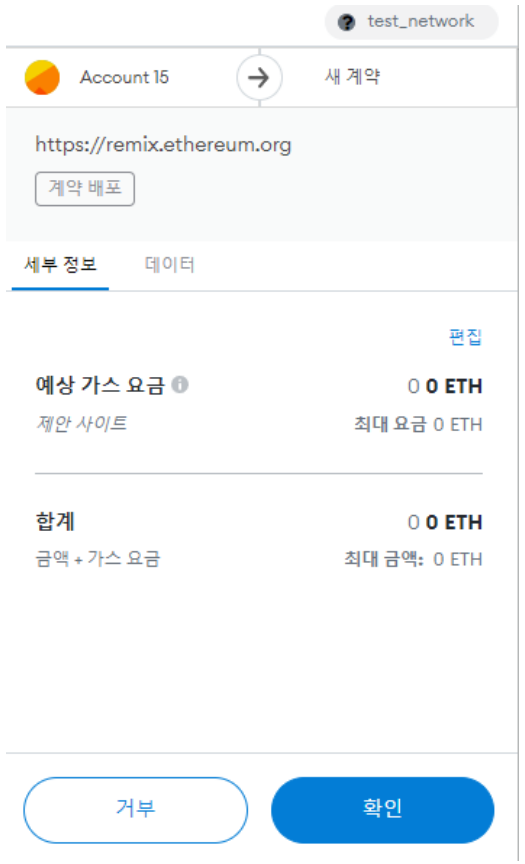

ENVIRONMENT
Injected Web3
Custom (1337) network
ACCOUNT
0x9D9...02325 (10200 ether)
GAS LIMIT
3000000
VALUE
0
Wei
CONTRACT
IERC20 - IERC20.sol
Deploy
Publish to IPFS

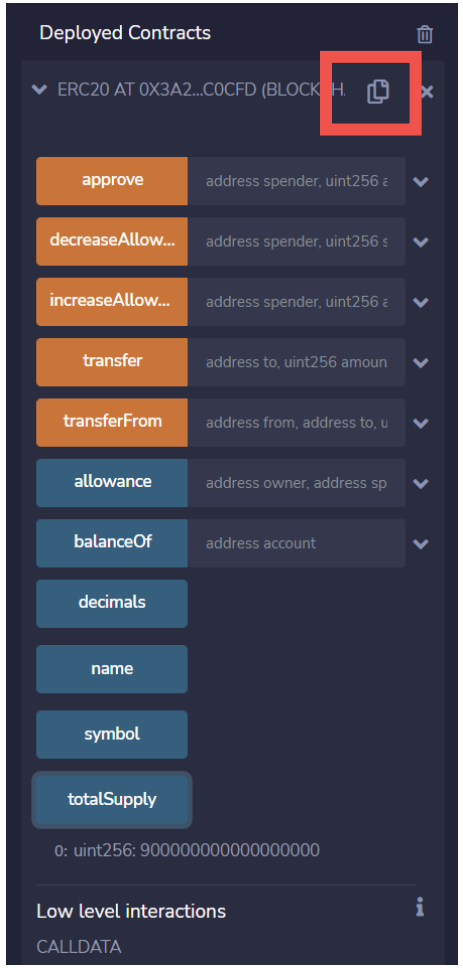

CONTRACT
ERC20 - ERC20.sol
DEPLOY
NAME_:
jw
SYMBOL_:
jw
MINT_:
900000000000000000
transact

토큰 발행 실습

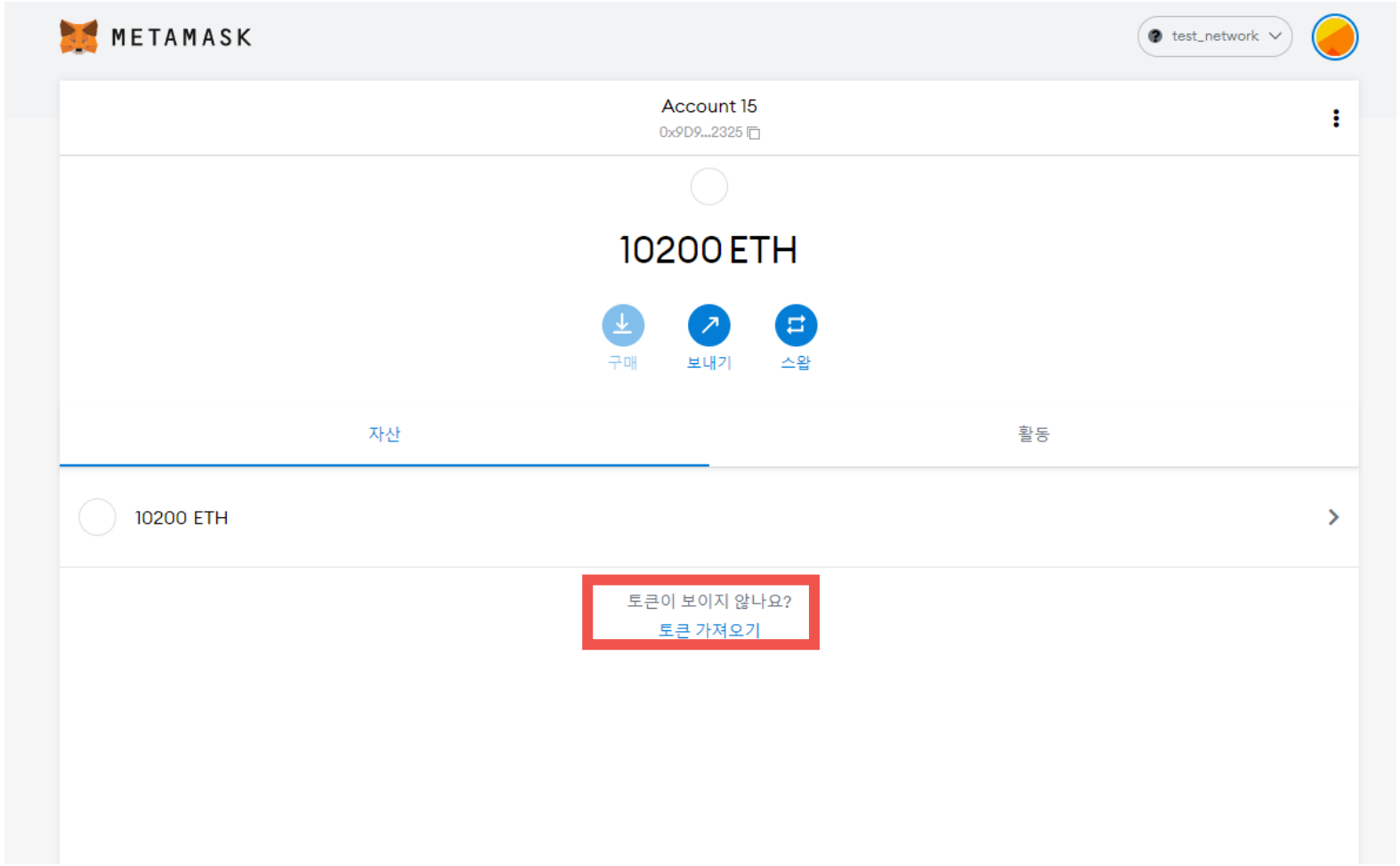
```
creation of ERC20 pending...
```

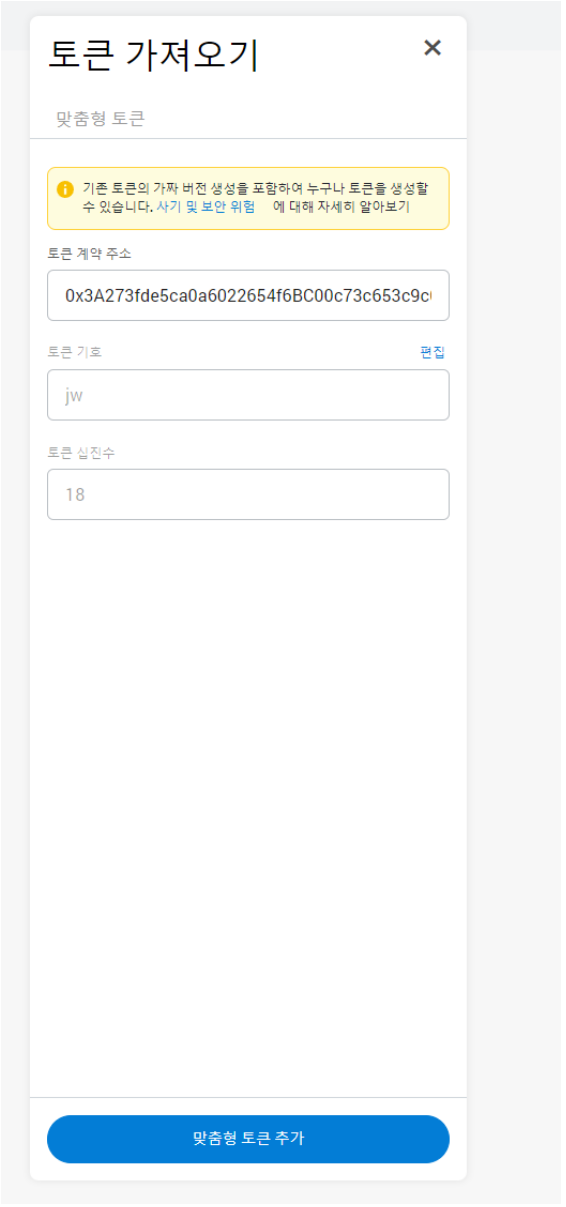




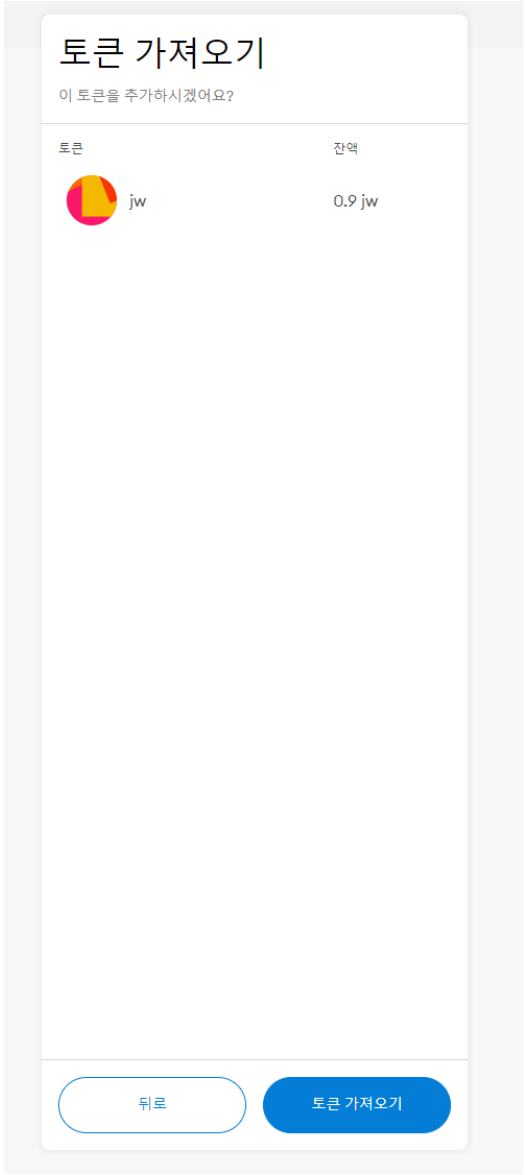


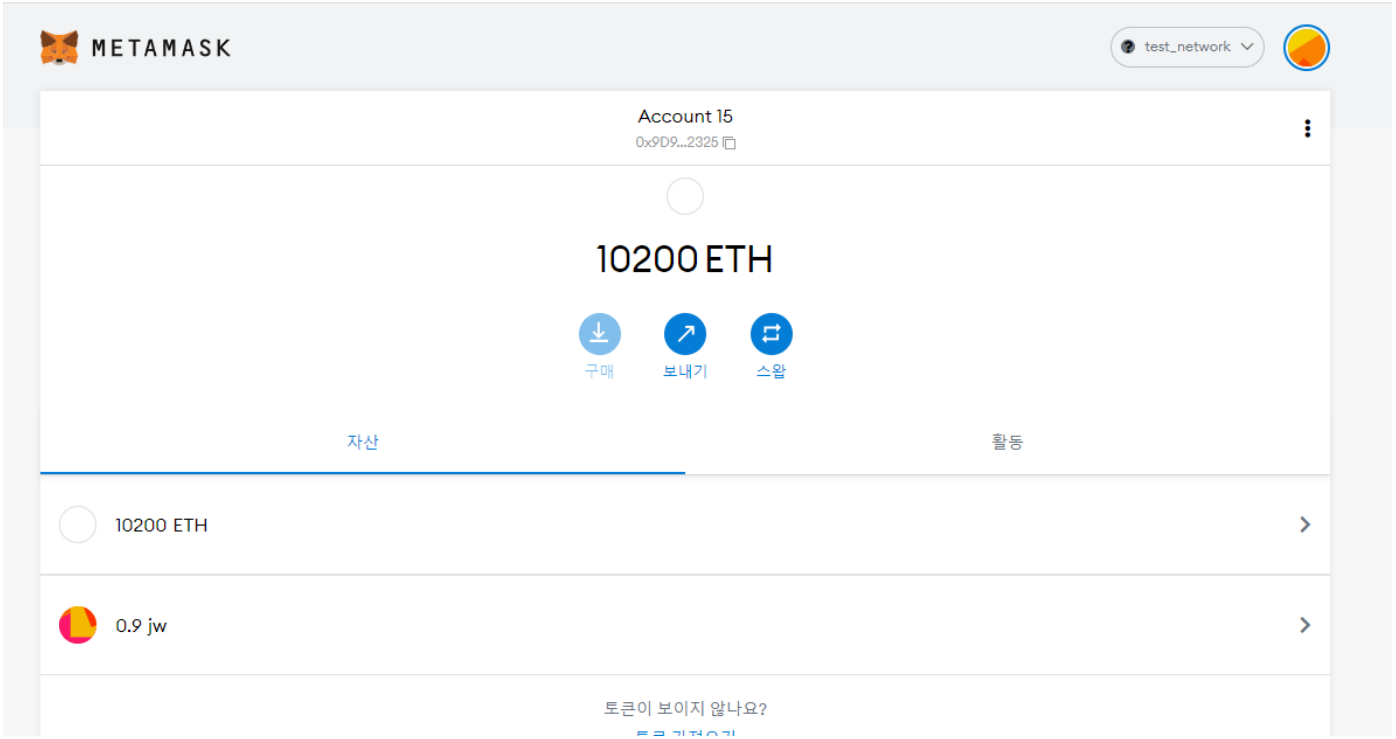
토큰 발행 실습


METAMASK
test_network
Account 15
0x9D9...2325
10200 ETH
구매
보내기
스왑
자산
활동
10200 ETH
토큰이 보이지 않나요?
토큰 가져오기


토큰 가져오기
맞춤형 토큰
기존 토큰의 가짜 버전 생성을 포함하여 누구나 토큰을 생성할 수 있습니다. 사기 및 보안 위험 에 대해 자세히 알아보기
토큰 계약 주소
0x3A273fde5ca0a6022654f6BC00c73c653c9c
토큰 기호
편집
jw
토큰 십진수
18
맞춤형 토큰 추가

토큰 발행 실습


토큰 가져오기
이 토큰을 추가하시겠어요?
토큰
잔액
jw
0.9 jw
뒤로
토큰 가져오기


METAMASK
test_network
Account 15
0x9D9...2325
10200 ETH
구매
보내기
스왑
자산
활동
10200 ETH
0.9 jw
토큰이 보이지 않나요?

목차

1. 실습 준비

1) 스마트 컨트랙트
2) 하이퍼렛저 베수 구동
3) Remix 활용
4) Web3 사용

2. 토큰 발행 실습

1) 토큰 발행 실습

3. 지갑 만들기

1) 지갑 만들기 실습

Nodejs 설치

```
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ node -v
v12.14.0
```

npm init

```
$ npm init
This utility will walk you through creating a package.json file.
It only covers the most common items, and tries to guess sensible defaults.

See `npm help json` for definitive documentation on these fields
and exactly what they do.

Use `npm install <pkg>` afterwards to install a package and
save it as a dependency in the package.json file.

Press ^C at any time to quit.
package name: (besu_wallet)
version: (1.0.0)
description:
entry point: (index.js)
test command:
git repository:
keywords:
author:
license: (ISC)
About to write to E:\besu_privateNetwork\besu_wallet\package.json:

{
  "name": "besu_wallet",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC"
}


Is this OK? (yes)
```

지갑 만들기 실습

package.json — E:₩besu_privateNetwork₩besu_wallet — Atom
File Edit View Selection Find Packages Help Debugger Nuclide
Project
besu_wallet
package.json
package.json
{
"name": "besu_wallet",
"version": "1.0.0",
"description": "",
"main": "index.js",
"scripts": {
"test": "echo \"Error: no test specified\" && exit 1"
},
"author": "",
"license": "ISC"
}

지갑 만들기 실습

npm install express

npm install web3

```
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ npm install express
npm notice created a lockfile as package-lock.json. You should commit this file.
npm WARN besu_wallet@1.0.0 No description
npm WARN besu_wallet@1.0.0 No repository field.

+ express@4.17.3
added 50 packages from 37 contributors and audited 50 packages in 3.332s

1 package is looking for funding
  run `npm fund` for details

found 0 vulnerabilities


system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ npm install web3
npm WARN deprecated request@2.88.2: request has been deprecated, see https://git
hub.com/request/request/issues/3142
npm WARN deprecated har-validator@5.1.5: this library is no longer supported
npm WARN deprecated multicodec@0.5.7: stable api reached

> bufferutil@4.0.6 install E:\besu_privateNetwork\besu_wallet\node_modules\buffe
rutil
> node-gyp-build


> secp256k1@4.0.3 install E:\besu_privateNetwork\besu_wallet\node_modules\secp25
6k1
> node-gyp-build || exit 0


> utf-8-validate@5.0.8 install E:\besu_privateNetwork\besu_wallet\node_modules\u
tf-8-validate
> node-gyp-build


> keccak@3.0.2 install E:\besu_privateNetwork\besu_wallet\node_modules\keccak
> node-gyp-build || exit 0


> web3-bzz@1.7.1 postinstall E:\besu_privateNetwork\besu_wallet\node_modules\web
3-bzz
> echo "WARNING: the web3-bzz api will be deprecated in the next version"

"WARNING: the web3-bzz api will be deprecated in the next version"

> web3-shh@1.7.1 postinstall E:\besu_privateNetwork\besu_wallet\node_modules\web
3-shh
> echo "WARNING: the web3-shh api will be deprecated in the next version"

"WARNING: the web3-shh api will be deprecated in the next version"

> web3@1.7.1 postinstall E:\besu_privateNetwork\besu_wallet\node_modules\web3
> echo "WARNING: the web3-shh and web3-bzz api will be deprecated in the next ve
rsion"

"WARNING: the web3-shh and web3-bzz api will be deprecated in the next version"
npm WARN besu_wallet@1.0.0 No description
npm WARN besu_wallet@1.0.0 No repository field.

+ web3@1.7.1
added 313 packages from 287 contributors and audited 363 packages in 26.807s

35 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

package.json　　package-lock.json

```
{
  "name": "besu_wallet",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.17.3",
    "web3": "^1.7.1"
  }
}
```

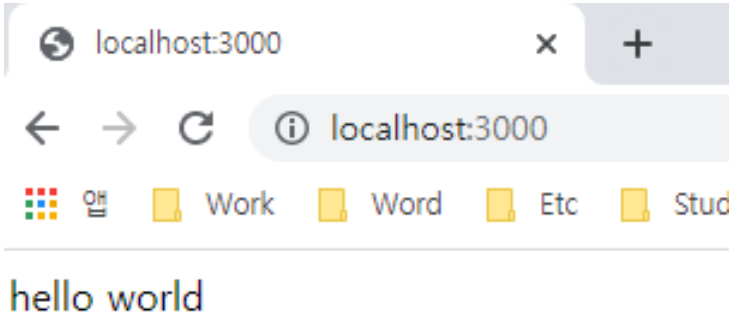
지갑 만들기 실습

server.js 파일 생성 후 작성

server.js

```
1  var express = require('express');
2  var app = express();
3
4  var server = app.listen(3000, function(){
5    console.log("server is working now")
6  })
7
8  app.get('/', function(req, res){
9    res.send('hello world')
10 })
```

```
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ node server.js
server is working now
```



지갑 만들기 실습

Html 페이지 만들기

package.json

```
{
  "name": "besu_wallet",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.17.3",
    "web3": "^1.7.1",
    "body-parser": "^1.19.0"
  }
}
```

```
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ npm install
npm WARN besu_wallet@1.0.0 No description
npm WARN besu_wallet@1.0.0 No repository field.

audited 364 packages in 1.836s

35 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
```

지갑 만들기 실습

Html 페이지 만들기

```
var express = require('express');
var app = express();
var bodyParser = require('body-parser');

app.use(bodyParser.json())
app.use(bodyParser.urlencoded({ extended: true}));


app.get('/', function(req, res){
  res.sendFile(__dirname+ "/index.html")
})

app.get('/deploy', function(req, res){
  res.sendFile(__dirname+ "/deploy.html")
})

var server = app.listen(3000, function(){
  console.log("server is working now")
})
```

server.js | deploy.html | index.html

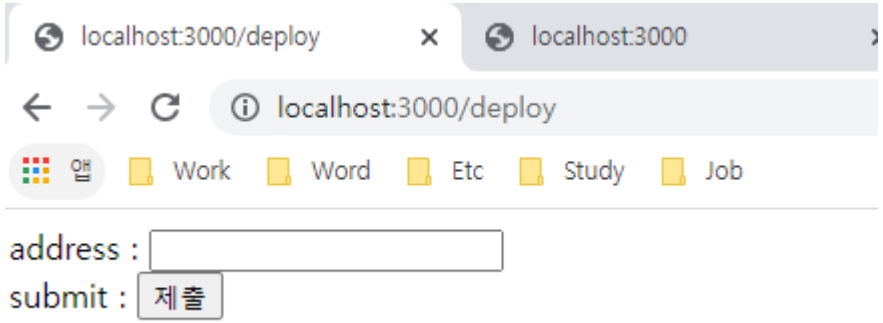
```
<form action="post" method="post">
  address : <input type="text" name="address" /><br />
  submit : <input type="submit" />
</form>
```

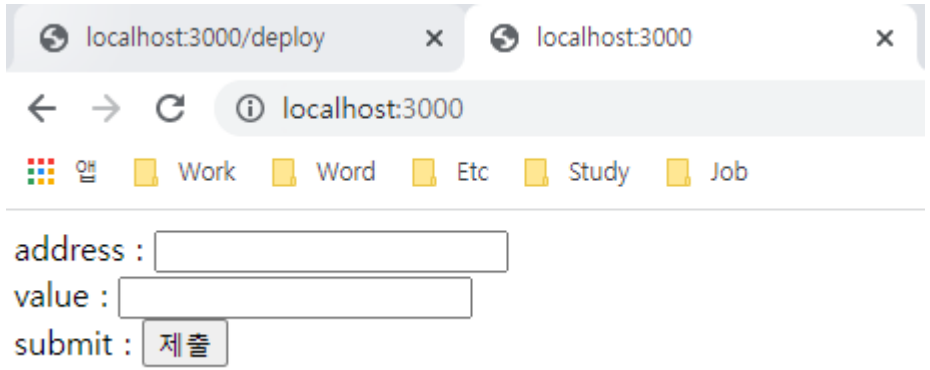
server.js | deploy.html | index.html

```
<form action="post" method="post">
  address : <input type="text" name="address" /><br />
  value : <input type="text" name="value" /> <br />
  submit : <input type="submit" />
</form>
```

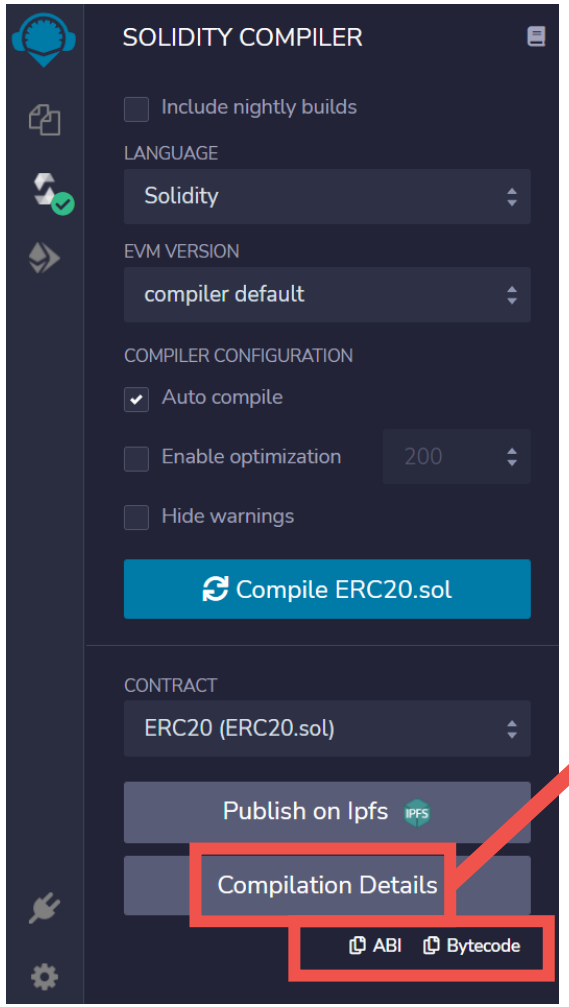
지갑 만들기 실습

Html 페이지 만들기



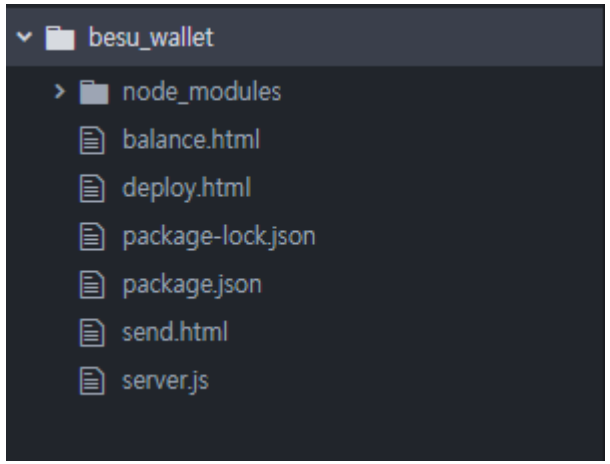


지갑 만들기 실습


SOLIDITY COMPILER
Include nightly builds
LANGUAGE
Solidity
EVM VERSION
compiler default
COMPILER CONFIGURATION
Auto compile
Enable optimization
200
Hide warnings
Compile ERC20.sol
CONTRACT
ERC20 (ERC20.sol)
Publish on Ipfs
Compilation Details
ABI
Bytecode

ERC20
METADATA
BYTECODE
ABI
WEB3DEPLOY
METADATAHASH
FUNCTIONHASHES
GASESTIMATES
DEVDOC
USERDOC
RUNTIME BYTECODE
ASSEMBLY

파일 및 package.json 내용




```json
{
  "name": "besu_wallet",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "test": "echo \"Error: no test specified\" && exit 1"
  },
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.17.3",
    "web3": "^1.7.1",
    "body-parser": "^1.19.0",
    "ethereumjs-tx": "^1.3.7"
  }
}
```

지갑 만들기 실습

Html 파일

deploy.html

```
<form action="/deploy" method="post">
  token_name: <input type="text" name="tn" /><br />
  token_symbol: <input type="text" name="ts" /><br />
  total_supply: <input type="text" name="supply" /><br />
  submit : <input type="submit" />
</form>
```

send.html

```
<form action="/send" method="post">
  address : <input type="text" name="address" /><br />
  value : <input type="text" name="value" /> <br />
  submit : <input type="submit" />
</form>
```

balance.html

```
<form action="/balance" method="post">
  address : <input type="text" name="address" /><br />
  submit : <input type="submit" />
</form>
```

지갑 만들기 실습

Server.js 파일

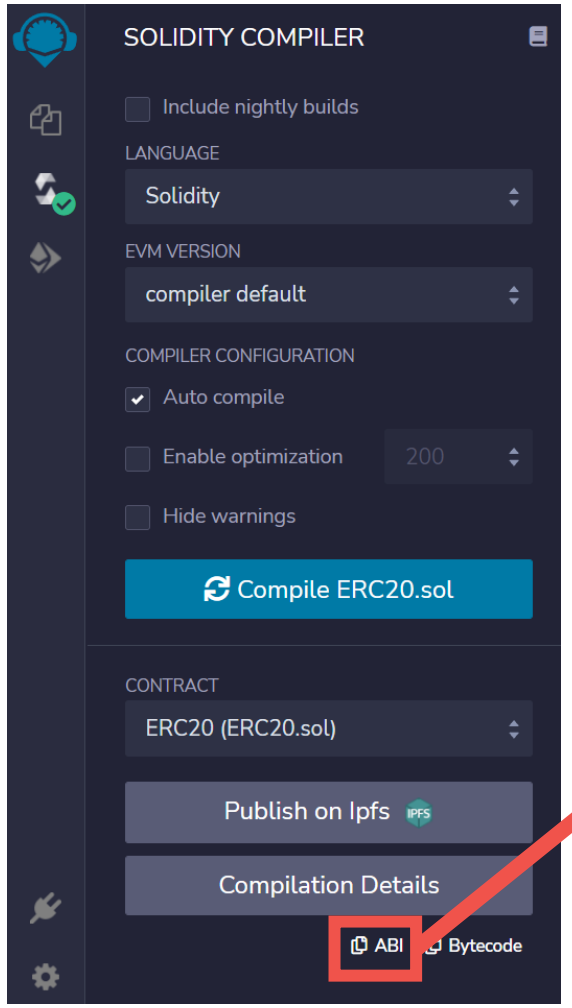
```
1  var express = require('express');
2  var app = express();
3  var bodyParser = require('body-parser');
4  var Web3 = require('web3');
5  var ethTx = require('ethereumjs-tx');
6
7  var web3 = new Web3(new Web3.providers.HttpProvider('http://127.0.0.1:8545'));
8
9  const address = '9D9a133eFE458949E30F6D4B184eD0CE11D02325'
10 const priv_key = Buffer.from('b628eda31d34b136633ff9d2b5177824569966560084768e0722df1e497ff773', 'hex');
```

Address 주소, 앞에 0x 제거

Private key 정보

지갑 만들기 실습

Server.js 파일



복사

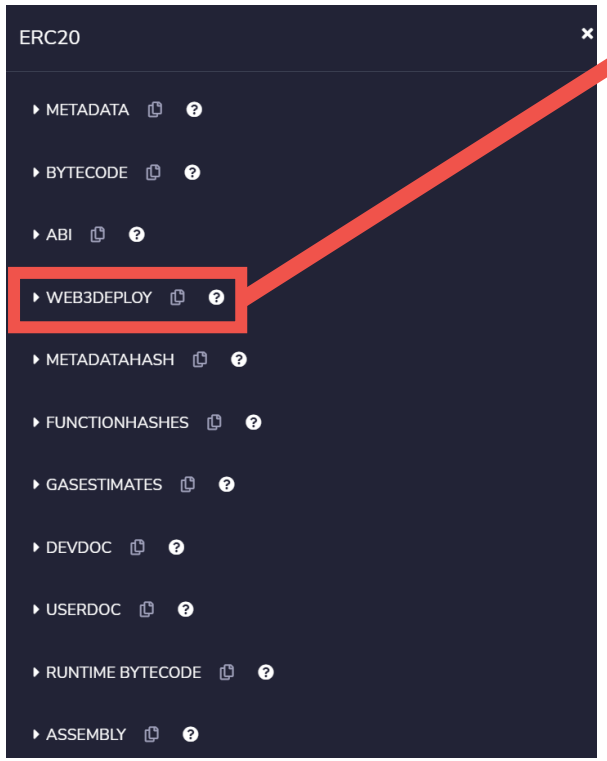
```
var ABI = [
{
  "inputs": [
    {
      "internalType": "string",
      "name": "name_",
      "type": "string"
    },
    {
      "internalType": "string",
      "name": "symbol_",
      "type": "string"
    },
    {
      "internalType": "uint256",
      "name": "mint_",
      "type": "uint256"
    }
  ],
  "stateMutability": "nonpayable",
  "type": "constructor"
},
{
  "anonymous": false,
  "inputs": [
    {
      "indexed": true,
      "internalType": "address",
      "name": "owner",
      "type": "address"
    },
    {
      "indexed": true,
      "internalType": "address",
      "name": "spender",
      "type": "address"
```

지갑 만들기 실습

Server.js 파일

```
309  app.use(bodyParser.json())
310  app.use(bodyParser.urlencoded({ extended: true}));
311
312
313
314  app.get('/deploy', function(req, res){
315    res.sendFile(__dirname+ "/deploy.html")
316  })
317
```

```
318  app.post('/deploy', function(req, res){
319      var name_ = req.body.tn;
320      var symbol_ = req.body.ts ;
321      var mint_ = req.body.supply;
```



복사

```
var erc20Contract = new
web3.eth.Contract([{"inputs":[{"internalType":"string","n
pe":"uint256"}],"name":"Approval","type":"event"},{"anony
nternalType":"uint256","name":"","type":"uint256"}],"stat
pe":"uint256"}],"stateMutability":"view","type":"function
ype":"address","name":"spender","type":"address"},{"inter
"view","type":"function"},{"inputs":[],"name":"totalSuppl
nternalType":"address","name":"to","type":"address"},{"in

var erc20 = erc20Contract.deploy({
   data:
   '0x608060405234801562000011576000 80fd5b506040516200194
   fd5b6200010b60008383620001fd60201b60201c565b8060026000
   36200020260201b60201c565b5050565b505050565b505050565b8
   565b7f4e487b7100000000000000000000000000000000000000000
   d620003e7846200036a565b6200034b565b905082815260208101 8
   0162000421565b935050602084015167ffffffffffffffff811115
   0000060005260116004526024 6000fd5b6000620005e8826200045
   565b5b50919050565b61126880620006db6000396000f3fe608060
   d565b610308565b6040516100f39190610c38565b6040518091039
   9190610b22565b60405180910390f35b6102006004803603810190
   16102fe565b820191906000526020600020905b815481529060010
   ffffffffffffffffffffffffffffffff168152602001908152602 0
   0000000000000000081526004016104d390610ecc565b604051809
   ffffffffffffffffff168373ffffffffffffffffffffffffffffff
   ffffffffffffffffffffffff168152602001908152602001600 2
   6107f857818110156107ea576040517f08c379a000000000000000
   fff1614156108de576040517f08c379a000000000000000000000
   ffffffffffffffffffffffffffff168152602001908152602001
   000815190509050565b60008282526020820190509291505056 5
   69565b8114610b8f57600080fd5b50565b600081359050610ba181
   15050565b60008060006060848603121561 0c9657610c95610b445
   9050565b7f4e487b7100000000000000000000000000000000000000
```

Server.js 파일

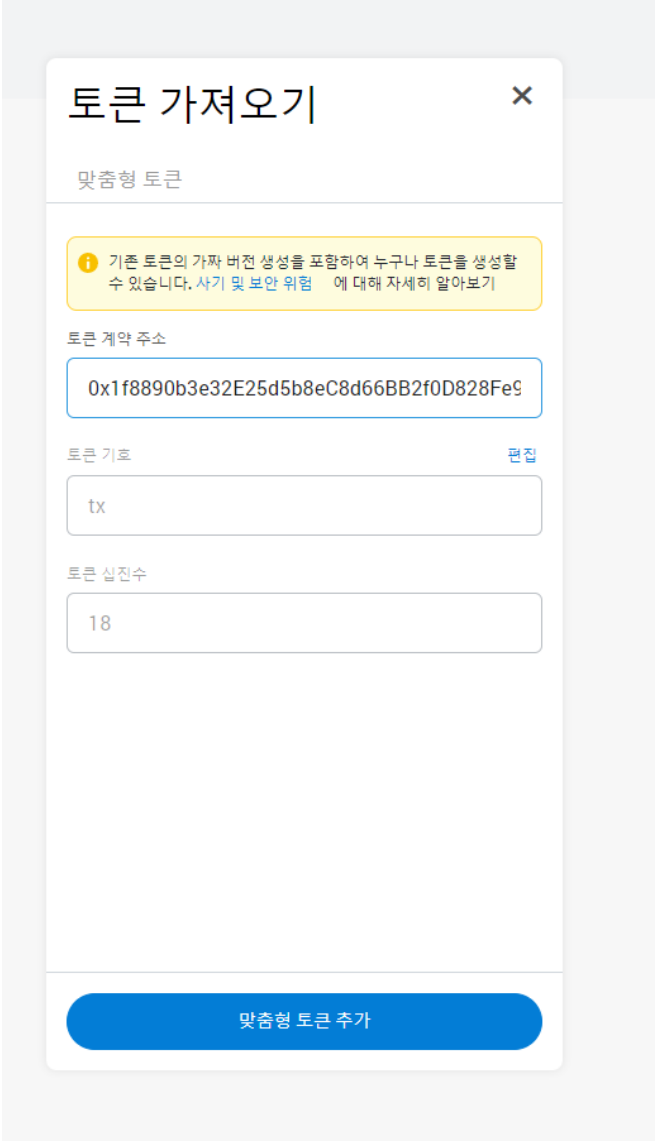
```
327         arguments: [
328             name_,
329             symbol_,
330             mint_,
331         ]
332     })
```

```
333
334     var set_string_byte_code = erc20.encodeABI();
335
336     web3.eth.getTransactionCount (address, "pending", (err, nonce) => {
337       var Raw_Tx = {
338         nonce: web3.utils.toHex(nonce),
339         gasPrice: web3.utils.toHex(1000),
340         gasLimit: web3.utils.toHex(3000000),
341         data: set_string_byte_code,
342         from: address
343       };
344
345       var Signature = new Buffer.from(priv_key, "hex");
346
347       var Make_Tx = new ethTx(Raw_Tx);
348       Make_Tx.sign(Signature);
349
350       var Serialized_Tx = Make_Tx.serialize();
351       var Raw_Tx_Hex = '0x' + Serialized_Tx.toString('hex');
352
353       web3.eth.sendSignedTransaction(Raw_Tx_Hex).on('receipt', receipt => {
354         console.log('receipt :', receipt);})
355
356   })
357
358   })
```

지갑 만들기 실습

Deploy 결과

```
system888@DESKTOP-GM35NPN MINGW64 /e/besu_privateNetwork/besu_wallet
$ node server.js
server is working now
receipt : {
  blockHash: '0xcfaa578d230259c3290ae3c9d766ce7b96186bc4ccb5eb884fa9d3d981ec0d9b
',
  blockNumber: 387
  contractAddress: '0x1f8890b3e32E25d5b8eC8d66BB2f0D828Fe9a384',
  cumulativeGasUsed
  from: '0x9d9a133efe458949e30f6d4b184ed0ce11d02325',
  gasUsed: 1179633,
  effectiveGasPrice: 1000,
  logs: [
    {
      address: '0x1f8890b3e32E25d5b8eC8d66BB2f0D828Fe9a384',
      topics: [Array],
      data: '0x0000000000000000000000000000000000000000000000000000000000000186a0'
,
      blockNumber: 3876,
      transactionHash: '0x5562289dddaa6d36be666833d32a5fb25b53c9c89650255cfb7d91
8cc4f97295',
      transactionIndex: 0,
      blockHash: '0xcfaa578d230259c3290ae3c9d766ce7b96186bc4ccb5eb884fa9d3d981ec
0d9b',
      logIndex: 0,
      removed: false,
      id: 'log_c43c10d4'
    }
  ],
  logsBloom: '0x0000000000000000000000000000000000000000000000000000000100000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000800000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000200000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000',
  status: true,
  to: null,
  transactionHash: '0x5562289dddaa6d36be666833d32a5fb25b53c9c89650255cfb7d918cc4
f97295',
  transactionIndex: 0
}
```



지갑 만들기 실습

Server.js 파일

```
360  app.get('/send', function(req, res){
361    res.sendFile(__dirname+ "/send.html")
362  })
363
364  app.post('/send', function(req, res){
365
366    var contract_address = "0x14B0Ce95857917aaB5Ab13aC6C0F7ec9fC611582";
367
368    var contract = new web3.eth.Contract(ABI, contract_address)
369
370    var set_contract = contract.methods.transfer(req.body.address, req.body.value);
371
372    var set_contract_byte = set_contract.encodeABI();
373
374    web3.eth.getTransactionCount (address, "pending", (err, nonce) => {
375      var Raw_Tx = {
376        nonce: web3.utils.toHex(nonce),
377        gasPrice: web3.utils.toHex(1000),
378        gasLimit: web3.utils.toHex(3000000),
379        data: set_contract_byte,
380        from: address,
381        to: contract_address
382      };
```

```
384      var Signature = new Buffer.from(priv_key, "hex");
385
386      var Make_Tx = new ethTx(Raw_Tx);
387      Make_Tx.sign(Signature);
388
389      var Serialized_Tx = Make_Tx.serialize();
390      var Raw_Tx_Hex = '0x' + Serialized_Tx.toString('hex');
391
392      web3.eth.sendSignedTransaction(Raw_Tx_Hex).on('receipt', receipt => {
393        console.log('receipt :', receipt);})
394
395  })
396
397
398  })
```

Deploy 이후 나타나는 Smart Contract address

Server.js 파일

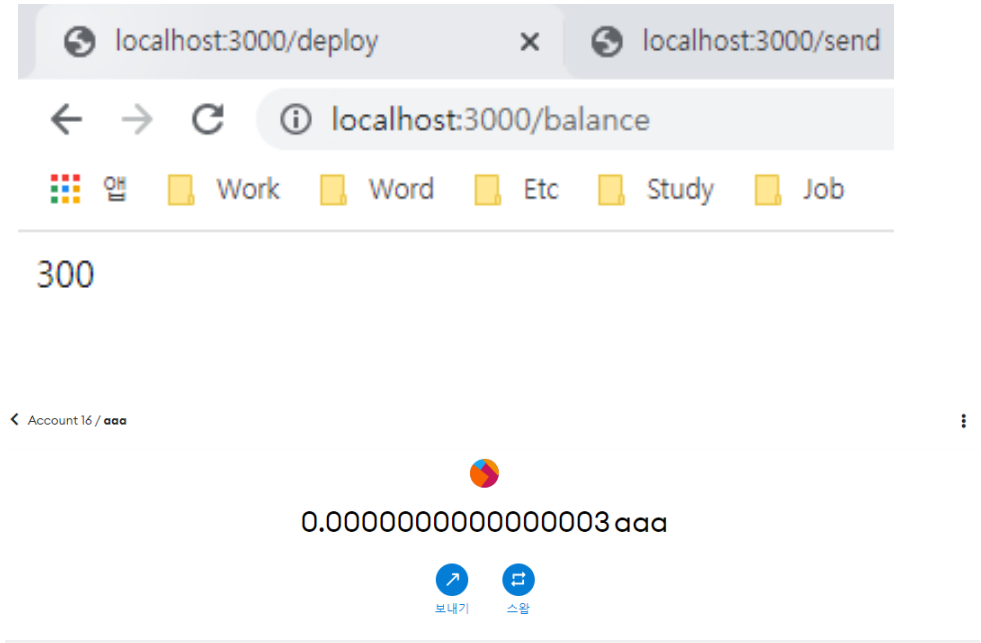
```
401  app.get('/balance', function(req, res){
402    res.sendFile(__dirname+"/balance.html")
403  })
404
405  app.post('/balance', function(req, res){
406    var contract_address = "0x14B0Ce95857917aaB5Ab13aC6C0F7ec9fC611582";
407    var contract = new web3.eth.Contract(ABI, contract_address);
408
409    contract.methods.balanceOf(req.body.address).call().then(data =>{
410
411      var decimal = Math.pow(10, 18)
412      var new_data = data / decimal
413
414      console.log(new_data);
415
416      res.send("balance= " +new_data)
417    })
418
419  })
420
421
422  var server = app.listen(3000, function(){
423    console.log("server is working now")
424  })
```

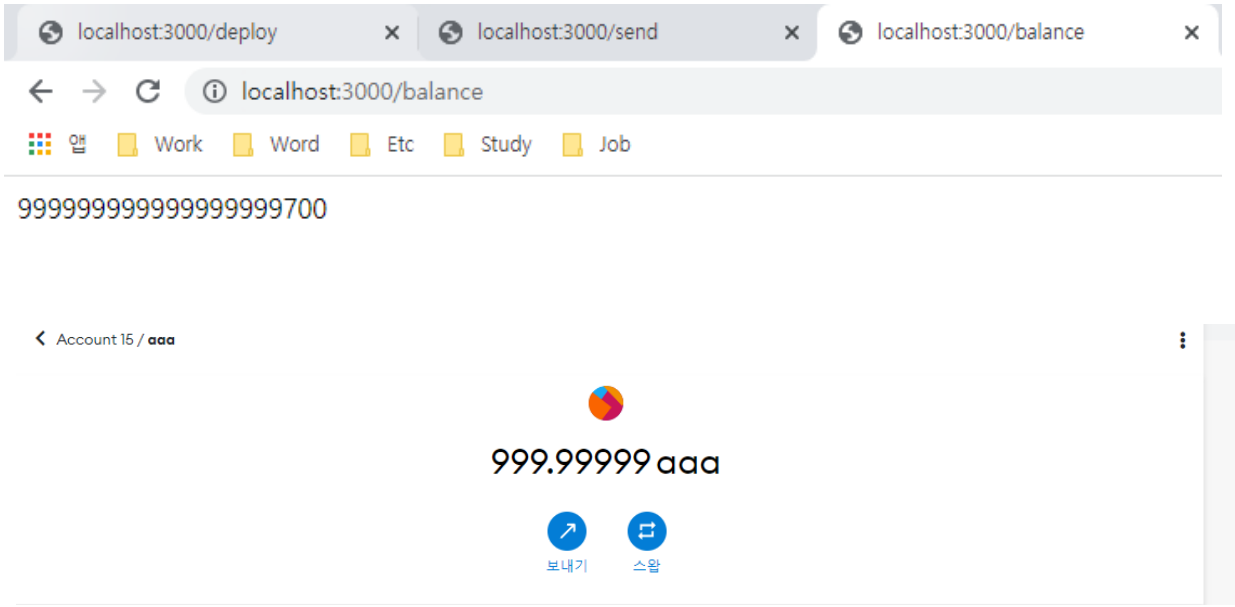
지갑 만들기 실습

```
receipt : {
  blockHash: '0xc4c2581f936e4a333d9c1e9295567117e3ea46f542ff4b8619adb6869c9f3765
',
  blockNumber: 7243,
  contractAddress: null,
  cumulativeGasUsed: 36833,
  from: '0x9d9a133efe458949e30f6d4b184ed0ce11d02325',
  gasUsed: 36833,
  effectiveGasPrice: 1000,
  logs: [
    {
      address: '0x14B0Ce95857917aaB5Ab13aC6C0F7ec9fC611582',
      topics: [Array],
      data: '0x0000000000000000000000000000000000000000000000000000000000000064'
,
      blockNumber: 7243,
      transactionHash: '0x53c0e926979b36c1c47a7d0468890bc103fabf7c14c10751c2ec9e
e104933076',
      transactionIndex: 0,
      blockHash: '0xc4c2581f936e4a333d9c1e9295567117e3ea46f542ff4b8619adb6869c9f
3765',
      logIndex: 0,
      removed: false,
      id: 'log_96ce6af2'
    }
  ],
  logsBloom: '0x0000000000000000000000000000000000000000000000000000000000000100000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000800000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0000000000
```

지갑 만들기 실습

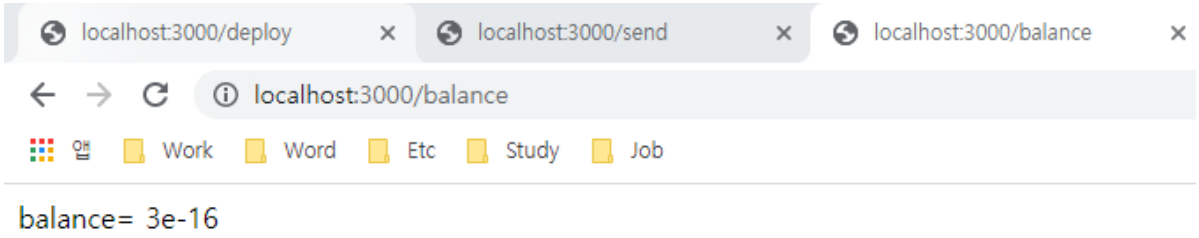
Balance 적용 완료
Decimal 적용 안된 상태

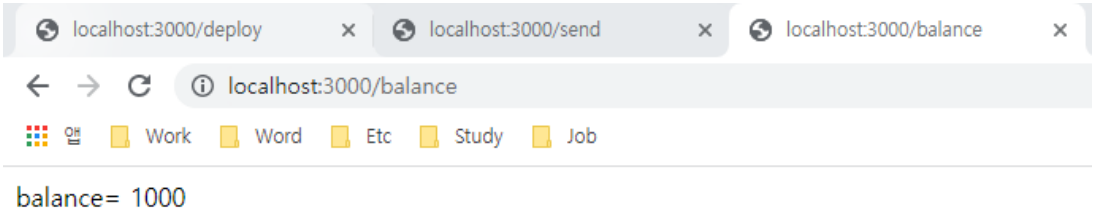


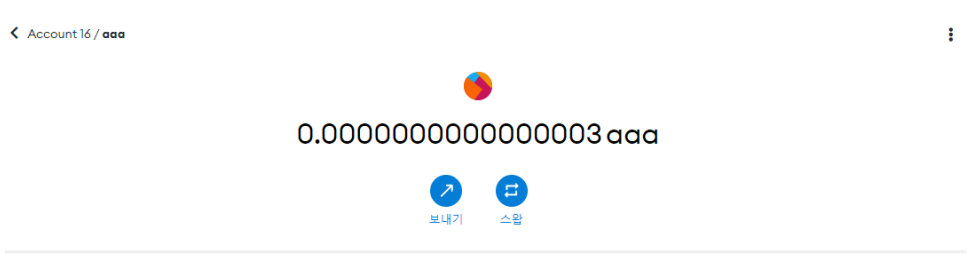


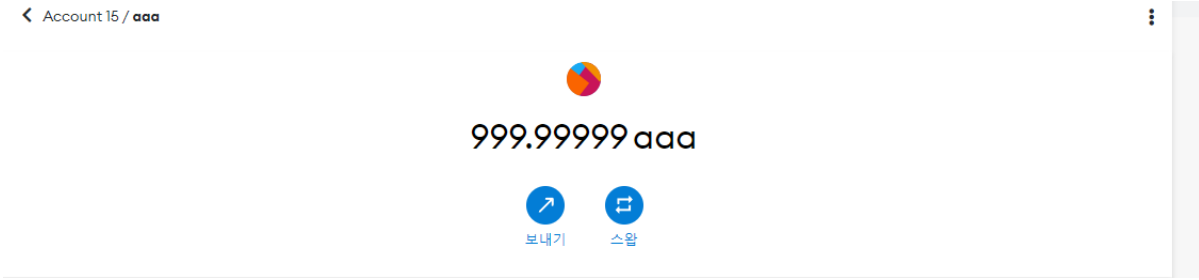
지갑 만들기 실습

Decimal 적용









지갑 만들기 실습

Decimal 해결법

```
    var decimal = Math.pow(10, 18)
    var new_data = data / decimal

    console.log(new_data);

    res.send("balance= " +new_data)
})
```

Nodejs 상에서 수식 Decimal 만큼 수식 적용

```
function decimals() public view virtual override returns (uint8) {
    return 18;
}
```

Smart contract상의 decimals 함수의 return 값
변경후 재 배포

Q & A