

스마트 컨트랙트 활용 실습



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 <ul style="list-style-type: none"> 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
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 상태 변수 읽기• this.balance 혹은 <주소>.balance 접근• Block, tx, msg중 하나의 멤버 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) {  
    }
```

```
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     }  
10 }
```

- 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 받았을 때 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
- modifier 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

privateNetwork > besu_network

이름

- networkFiles
- node1
- node2
- node3
- node4
- command.txt
- genesis.json
- genesis_creator.json



하이퍼렛저 벡수 구동

```
MINGW64/c:/besu/privateNetwork/besu_network/node1
[...]
```

```
MINGW64/c:/besu/privateNetwork/besu_network/node2
[...]
```

```
MINGW64~/esu_privateNetwork/besu_network/node3
20d4e4a95df2e4782ab7c3ced45fcd803d331ea96e2db3bb281ef...updateAddress-Optional (/f27
1303051...msb4e4...ef00292f...
70k34jMoKvTusYmSgysE10tU7HwX0V3cs...GMRyGOJL4lR1MSumF3f7GSG-Gd5F2QV0A
FGHFdsCEAgmlgnYogmLWHHAAAGCZVJCdI1mesko76ELgAKKKkvja1-Vghlt8t8OBHXbcNGTUqGo
...node3...gwongZh...mode=prod...
6411990fdcf70eb73811...ethid={tcp:30303}...updateAddress-Optional (/f27
0022-03-06 12:22:14, 374:09:00 | main | INFO | DefaultTargetManager | Node address
x52baed1dc713c375f784d1990fdcf70eb738
022-03-06 12:22:14, 687:09:00 | main | INFO | DefaultSyncronizer | Starting sy
sync.
022-03-06 12:22:14, 730:09:00 | main | INFO | FullSyncDownloader | Startin
sync.
022-03-06 12:22:14, 374:09:00 | main | INFO | FullSyncTargetManager | No sync t
get, waiting for peers. Current peers: 0
022-03-06 12:22:14, 687:09:00 | main | INFO | Runner | Ethereum main loop is up
022-03-06 12:22:14, 790:09:00 | main | INFO | nioEventLoopGroup-3-4 | INFO | FullSyncTargetMa
No sync target, waiting for peers. Current peers: 3
MINGW64~/esu_privateNetwork/besu_network/node4
Schedule created with milestones: [MiningGlacier: 0]
022-03-06 12:22:14, 568:09:00 | main | INFO | RunnerBuilder | Detecting NAT ser
vice.
022-03-06 12:22:14, 702:09:00 | main | INFO | Runner | Starting external service
022-03-06 12:22:14, 705:09:00 | main | INFO | WebSocketService | Starting Webso
cket service on 127.0.0.1:8548
022-03-06 12:22:14, 705:09:00 | vert.x-eventloop-thread-1 | INFO | WebSocketSer
vice | WebSocket service started and listening on 127.0.0.1:8548
022-03-06 12:22:15, 470:09:00 | main | INFO | AutoTransaction BloomCachingService
Starting auto transaction bloom caching service.
022-03-06 12:22:15, 470:09:00 | main | INFO | Metadata | Lookup ca
the metadata file in data directory: E:\besu_privateNetwork\besu_network\node4\data\cache
022-03-06 12:22:15, 484:09:00 | main | INFO | Runner | Starting Ethereum main l
oop ...
022-03-06 12:22:15, 484:09:00 | main | INFO | NATService | No NAT environment d
etected so no service could be started
022-03-06 12:22:15, 485:09:00 | main | INFO | NetworkRunner | Starting Network
022-03-06 12:22:15, 491:09:00 | mioEventLoopGroup-2-1 | INFO | RlpExchange | P2P
started on /ip4/0.0.0.0/tcp/30306
022-03-06 12:22:15, 492:09:00 | main | INFO | PeerDiscoveryAgent | Starting pee
r discovery agent on host=0.0.0.0, port=30306
```

[illegible]

```

MINGW64/E:/besu_privateNetwork/besu_network/node4
C:\schedule created with milestones: [MurGlacier: 0]
2022-03-06 12:22:42.9568+09:00 | main | INFO | RunnerBuilder | Detecting NAT ser-
vice.
2022-03-06 12:22:42.9470+09:00 | main | INFO | Runner | Starting external ser-
vice.
2022-03-06 12:22:42.9470+09:00 | main | INFO | WebsocketService | Starting Webso-
cket service on 127.0.0.1:8548
2022-03-06 12:22:50.1460+09:00 | vert.x-eventloop-thread-1 | INFO | WebsocketSer-
vice | Websocket service started and listening on 127.0.0.1:8548
2022-03-06 12:22:50.470+09:00 | main | INFO | AutoTransactionGloomCacheServing-
Service | Starting auto transaction bloom caching service
2022-03-06 12:22:50.470+09:00 | main | INFO | CacheMetadata | Looking up ca-
che metadata file in data directory: E:/besu_privateNetwork/besu_network/node4/d-
ata/caches
2022-03-06 12:22:50.484+09:00 | main | INFO | Runner | Starting Ethereum main-
loop ...
2022-03-06 12:50.484+09:00 | main | INFO | NatService | No NAT environment d-
iscovered, no service could be started
2022-03-06 12:50.485+09:00 | main | INFO | NetworkRunner | Starting Network.
2022-03-06 12:52:50.491+09:00 | nioEventLoopGroup-2-1 | INFO | RlpXapp | P2P
started on 127.0.0.1:30306
2022-03-06 12:52:50.492+09:00 | main | INFO | PeerDiscoveryAgent | Starting pee-
r discovery agent on host=0.0.0.0, port=30306

```

```

MINGW64/e:/besu_privateNetwork/besu_network/node1
ntrollerBuilder | Produced #855 | 0 tx | 0 pending | 0 (0.0%) gas | (0xe1370b6d
29011cd78b9b9c9be34943bbf6e3415ff3bc5278517de7f51344)
2022-03-06 12:23:07.414+01:00: [INFO] EtlScheduler-Workers-0 | Persist8tBlockTas
t | Imported #856 | 0 tx | 0 om | 0 (0.0%) gas | (0x5ae77fa397ac83be948e6b9b676
57101fc89d6f454123ddb6b1c2ff0a53bf37) in 0.011s. Peers: 3
2022-03-06 12:22:59.253+01:00: [BftProcessorExecutor-IBFT-0] | INFO | IbfTsBesuC
ntrollerBuilder | Imported #856 | 0 tx | 0 pending | 0 (0.0%) gas | (0x5ae77fa39
7ac83be948e6b9b67657101fc89d6f454123ddb6b1c2ff0a53bf37)
2022-03-06 12:23:01.255+01:00: [BftProcessorExecutor-IBFT-0] | INFO | IbfTsBesuC
ntrollerBuilder | Imported #857 | 0 tx | 0 pending | 0 (0.0%) gas | (0x7206b535
a36037c613a51bdf1f7c349de5be9c21bfb5f6e6adC7041ba2b013)
2022-03-06 12:23:03.124+01:00: [BftProcessorExecutor-IBFT-0] | INFO | IbfTsBesuC
ntrollerBuilder | Imported #858 | 0 tx | 0 pending | 0 (0.0%) gas | (0x772f8c37
914787b1309d2a31055f974f37c019604b4f3cd2c062919e1ad84d)
2022-03-06 12:23:05.141+01:00: [BftProcessorExecutor-IBFT-0] | INFO | IbfTsBesuC
ntrollerBuilder | Produced #859 | 0 tx | 0 pending | 0 (0.0%) gas | (0xca7a8d32
914787b1309d2a31055f974f37c019604b4f3cd2c062919e1ad84d)
2022-03-06 12:23:07.247+01:00: [BftProcessorExecutor-IBFT-0] | INFO | IbfTsBesuC
ntrollerBuilder | Imported #860 | 0 tx | 0 pending | 0 (0.0%) gas | (0xb823b657
dcd25c8aee2381a0a651c4e00d46f8453fcd9a9006dbdf243bad6)
2022-03-06 12:23:07.247+01:00: [EtlScheduler-Workers-2] | INFO | Persist8tBlockTas
t | Imported #860 | 0 tx | 0 om | 0 (0.0%) gas | (0xb823b657dcd25c8aee2381a0a651
1c4e00d46f8453fcd9a9006dbdf243bad6) in 0.010s. Peers: 3

```

```
MINGW64~/e/besu_privateNetwork/besu_network/node3
```

controllerBuilder	Imported #854 / 0 tx / 0 pending / 0 (0.0%) gas /	(0x4ee72cfcb677a2f28a652c62b9dbd8f9454781e39c6af4d345d2cbbca533)
2022-03-06 12:22:57.253+00:00	BftProcessorExecutor-IBFT-0	INFO IabtBesuCo
b677a2f28a652c62b9dbd8f9454781e39c6af4d345d2cbbca533	Imported #855 / 0 tx / 0 pending / 0 (0.0%) gas /	(Iabt370b6dc901cd79b99e9cbe5eb943bfbc63415ff3f72b785f7371434)
2022-03-06 12:22:59.196+00:00	BftProcessorExecutor-IBFT-0	INFO IabtBesuCo
controllerBuilder	Produced #856 / 0 tx / 0 pending / 0 (0.0%) gas /	(0x5ae77f39a7ac83be94866b9b676e57101fc89de6f454123ddbb61c2ff0as3bf37)
2022-03-06 12:23:01.257+00:00	BftProcessorExecutor-IBFT-0	INFO IabtBesuCo
controllerBuilder	Imported #857 / 0 tx / 0 pending / 0 (0.0%) gas /	(0x7206b53571da4781431414014af25e0e5e2542febe90d1612982a74488b1)
2022-03-06 12:23:03.119+00:00	BftProcessorExecutor-IBFT-0	INFO IabtBesuCo
controllerBuilder	Imported #858 / 0 tx / 0 pending / 0 (0.0%) gas /	(0x772f8c371e14787b1309d2a3105f974f37c041960ab4f3cd2c062e919ead84d)
2022-03-06 12:23:05.146+00:00	BftProcessorExecutor-IBFT-0	INFO IabtBesuCo
controllerBuilder	Imported #859 / 0 tx / 0 pending / 0 (0.0%) gas /	(0xcaa7a8d320eb71da4781431414014af25e0e5e2542febe90d1612982a74488b1)
2022-03-06 12:23:05.155+00:00	EthScheduler-Workers-0	INFO PersistBlockTas

```
25e07ee5e2542febe90d1612982a74488b1) in 0.001s. Peers: 4  
2022-03-06 12:23:07.221+00:00 BftProcessorExecutor-IBFT-0 INFO | IabtBesuCo  
controllerBuilder Produced #860 / 0 tx / 0 pending / 0 (0.0%) gas /  
d25c8a8c2381a0a65b91cd4e000d4f87a53fcd9a0906bd724b3ade)
```

```

MINGW64:~/beshu/vateNetwork/beshu/network/node2
k | Imported 8856 / 0 tx / 0 om / 0 (0.0%) gas / (0x5ae77f3a97ac83be9486b9b67e
2022-03-06 12:23:00, 234+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfTBeSuC
ntrollerBuilder | Imported 8856 / 0 tx / 0 pending / 0 (0.0%) gas / (0x5ae77f3a9
7ac83be9486b9b67e57101fC89d6f454123dbd6b12cFf0a53bf37)
2022-03-06 12:23:01, 263+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfTBeSuC
ntrollerBuilder | Imported 8857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a1bdf17f3c49desbe93c21bbf566eac7041ba2b0b13)
2022-03-06 12:23:01, 263+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfTBeSuC
ntrollerBuilder | Produced 8858 / 0 tx / 0 pending / 0 (0.0%) gas / (0x772f8c371
914787b1309d2a31055f974f37c041960d4b3f3cd2062e9191eald84d)
2022-03-06 12:23:05, 149+09:00 | EthScheduler-Workers-2 | INFO | PersistBlockTas
k | Imported 8859 / 0 tx / 0 om / 0 (0.0%) gas / (0xca7a8d3201b71daaa41341ab10414
f25e07ee5e2542feb9e0d1612982a74488b1) in 0.005s. Peers: 4
2022-03-06 12:23:05, 149+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfTBeSuC
ntrollerBuilder | Imported 8859 / 0 tx / 0 pending / 0 (0.0%) gas / (0xca7a8d320
1b71daaa41341ab10414f25e07ee5e2542feb9e0d1612982a74488b1)
2022-03-06 12:23:07, 234+09:00 | EthScheduler-Workers-0 | INFO | PersistBlockTas
k | Imported 8860 / 0 tx / 0 om / 0 (0.0%) gas / (0xb823b657dcd25c8ace2381a0a65b
2022-03-06 12:23:07, 234+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfTBeSuC
ntrollerBuilder | Imported 8860 / 0 tx / 0 pending / 0 (0.0%) gas / (0xb823b657
cd25c8ace2381a0a65b91c4e000d4f6a533fcd4a90096d72f4b3ad6)

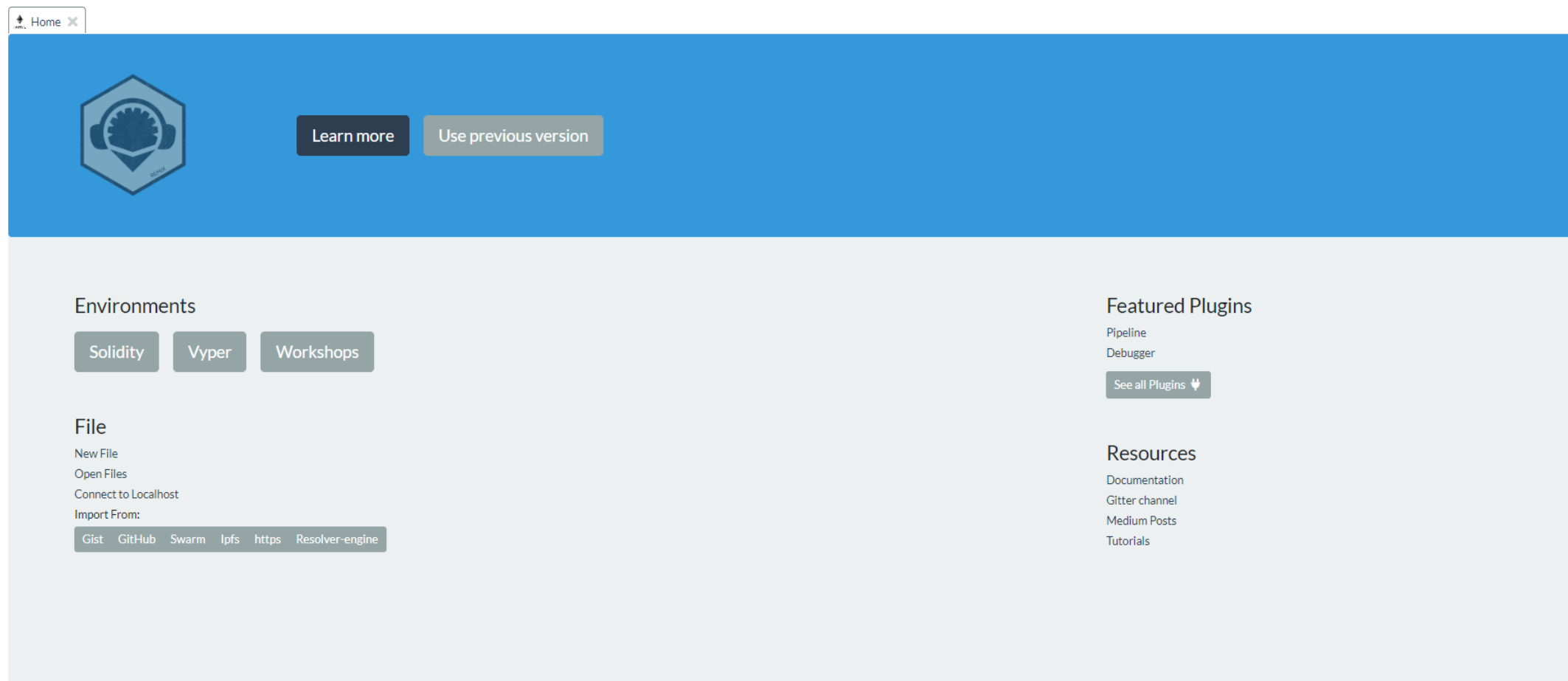
```

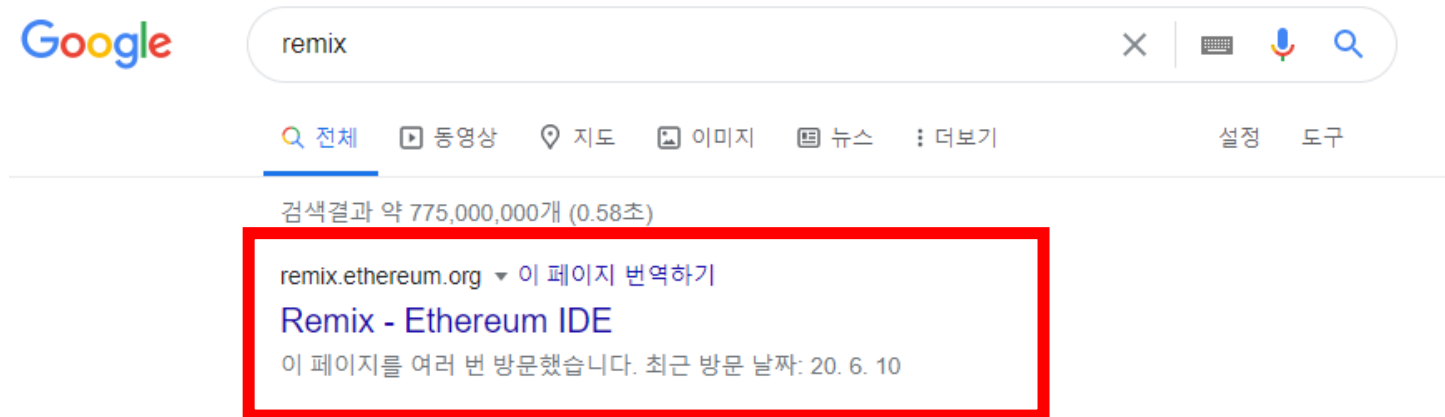
```

MINGW64: ~/esu_privateNetwork/besu_network/node4
c43b0b7be83415f35c2b78571dde7751434 in 0.000s. Peers: 4
2022-03-06 12:22:57.422+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #856 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox1370b6dc
29011cd789b99c9be5b
29011cd789b99c9be5b | c43b0b7be83415f35c2b78571dde7751434 in 0.000s. Peers: 4
2022-03-06 12:22:59.221+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #856 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox5ae77f3a9
7ac83be948e6b9676e57101fc89d6f454123dbd6b1c2ff0a53bf3f7
2ac83be948e6b9676e57101fc89d6f454123dbd6b1c2ff0a53bf3f7 in 0.000s. Peers: 4
2022-03-06 12:23:01.244+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #856 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox7206b5357
a36037c613a51bdf174949de5be9c9211b5f66a6d7041b2b013
a36037c613a51bdf174949de5be9c9211b5f66a6d7041b2b013 in 0.000s. Peers: 4
2022-03-06 12:23:03.133+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #856 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox772f8c371
914787b1309d2a31055f974f37c04a0064bf3cd2c062e919e1ad84d
914787b1309d2a31055f974f37c04a0064bf3cd2c062e919e1ad84d in 0.000s. Peers: 4
2022-03-06 12:23:03.133+09:00 | EthScheduler-Workers-1 | INFO | PersistBlockTas
ck | Imported #858 | 0 tx / 0 om / 0 (0.0%) gas / (Ox72f83c71914787b1309d2a31055
f974f37c04a0064bf3cd2c062e919e1ad84d in 0.000s. Peers: 4
2022-03-06 12:23:05.135+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #860 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox1370b6dc
29011cd789b99c9be5b
29011cd789b99c9be5b | c43b0b7be83415f35c2b78571dde7751434 in 0.000s. Peers: 4
2022-03-06 12:23:07.210+09:00 | BFTProcessorExecutor-IBFT-0 | INFO | IbfTbsuQc
ntrollerBuilder | Imported #860 | 0 tx / 0 pending / 0 (0.0%) gas / (Ox823b657c
cd25c8aec2381a0a65b91ce000d4f87a53fcd9a0096d724b3ad6)

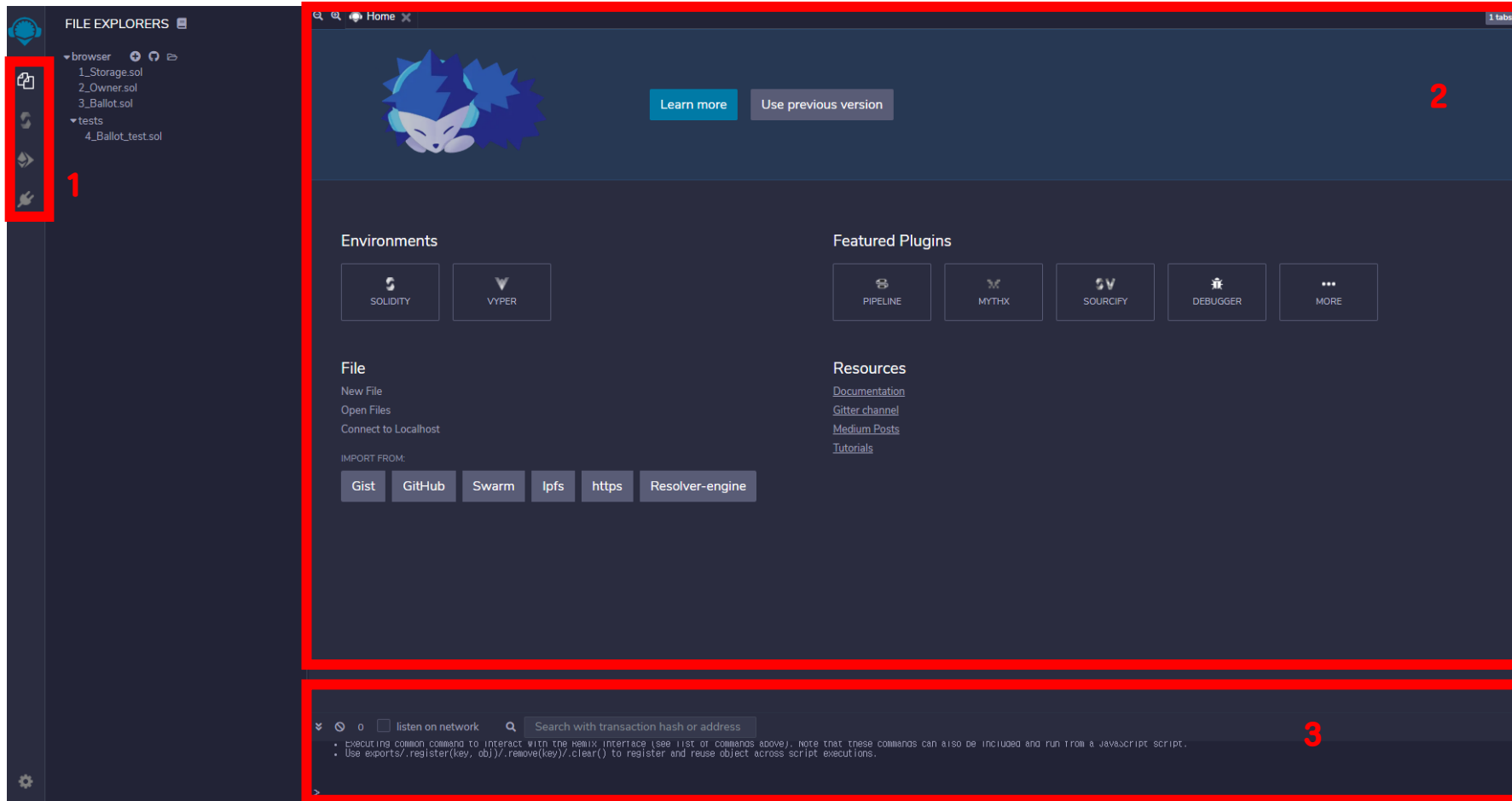
```

<https://remix.ethereum.org/>





Remix 활용

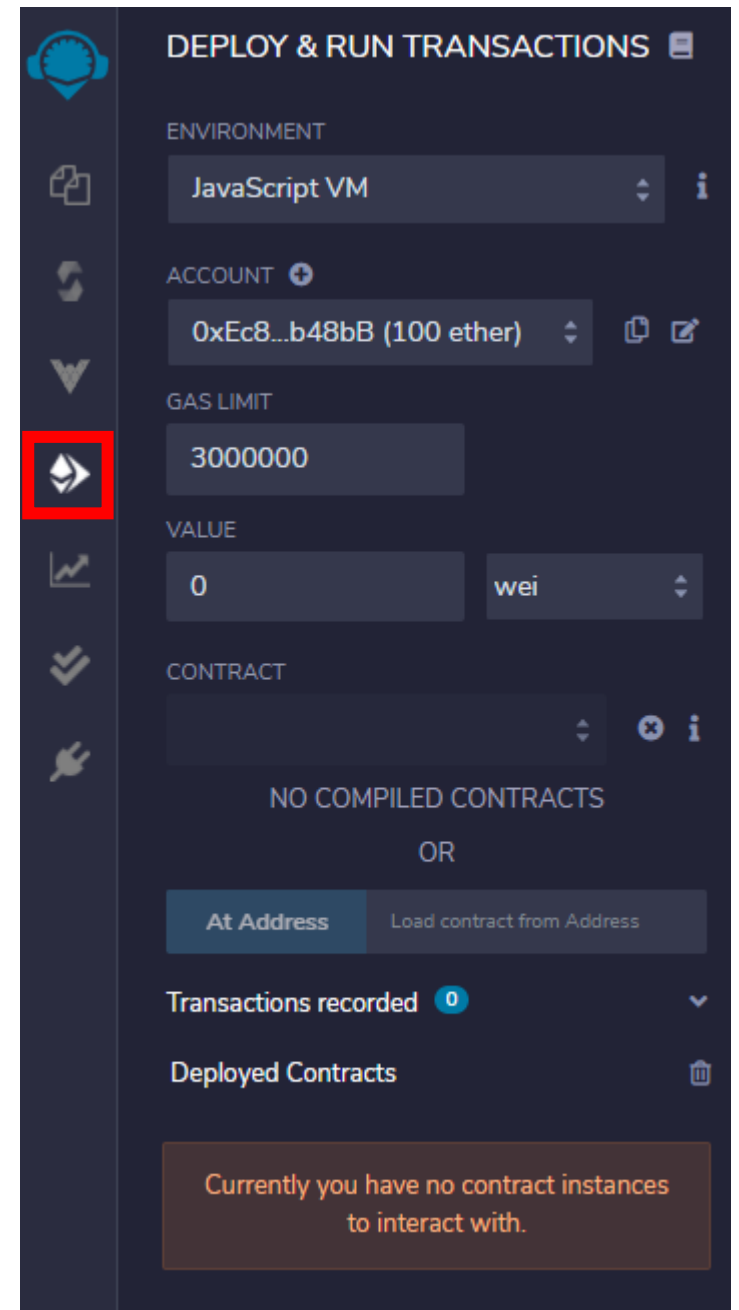
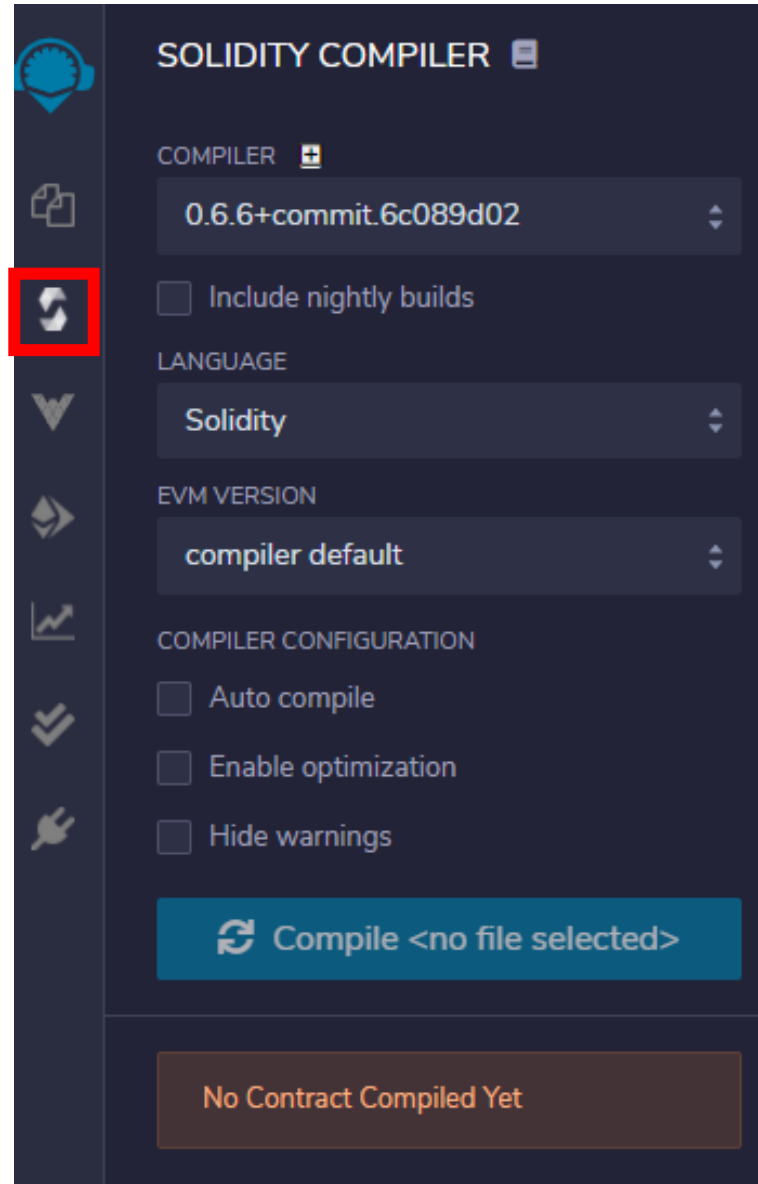
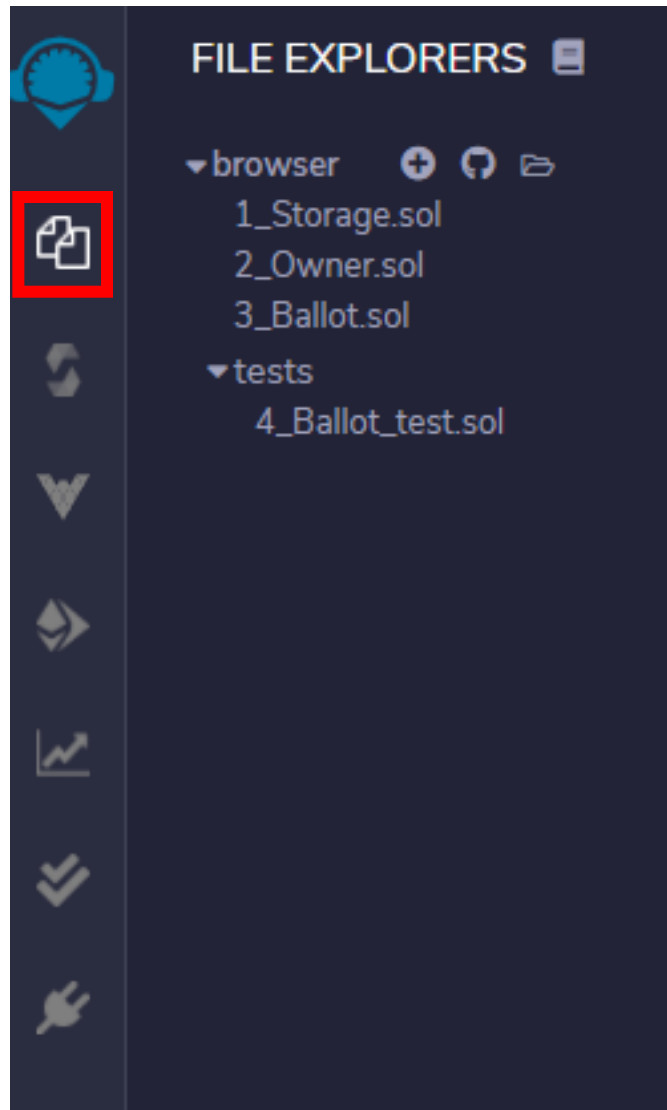


1. 탭

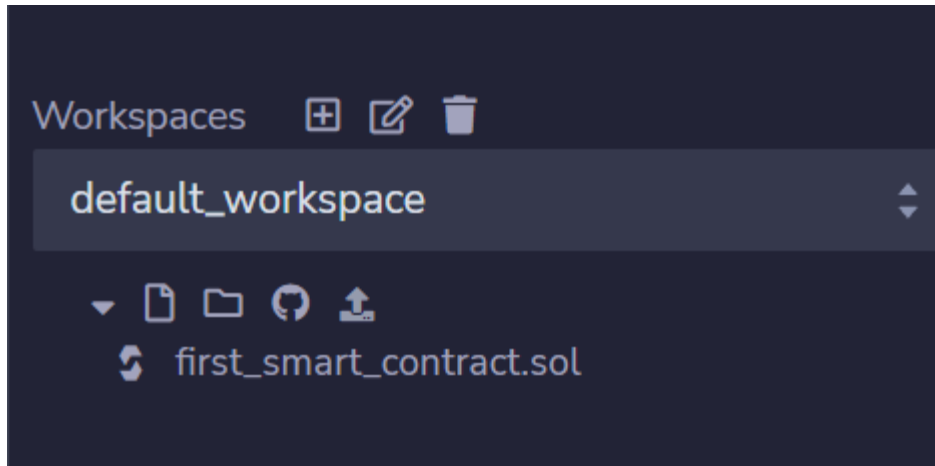
2. 메인 화면

3. 콘솔 화면

Remix 활용

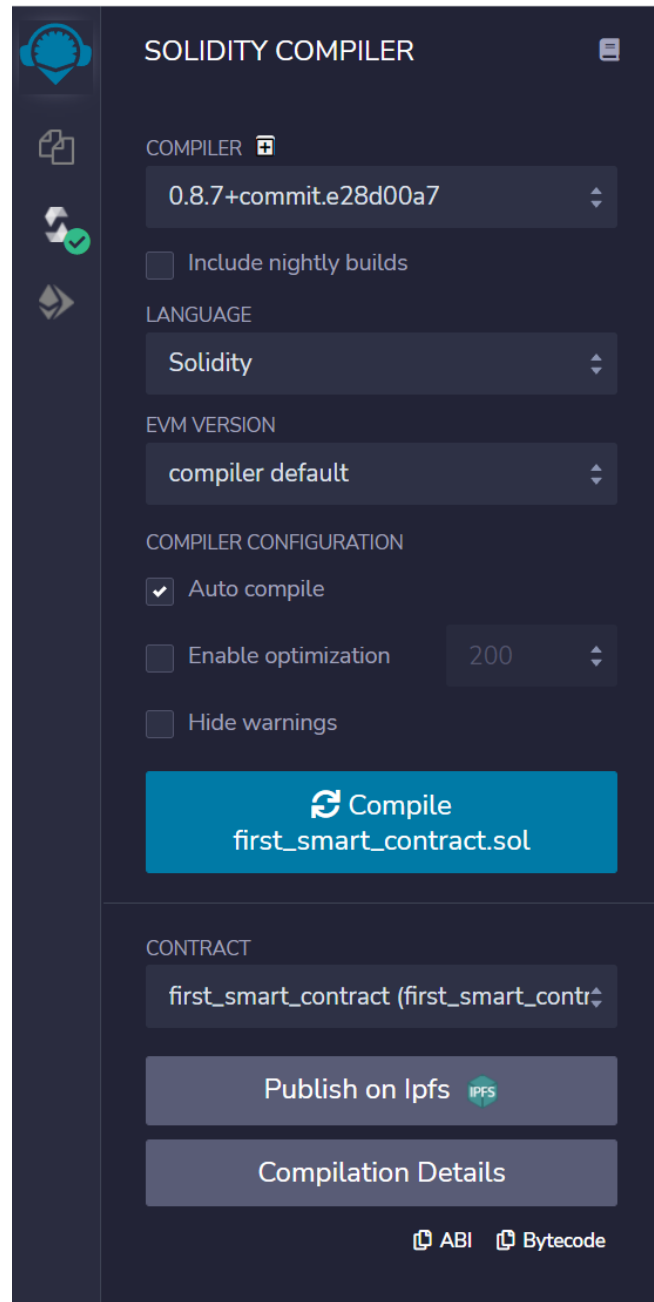


Remix 활용



```
1 // SPDX-License-Identifier: GPL-3.0
2
3 pragma solidity >=0.7.0 <0.9.0;
4
5 contract first_smart_contract {
6
7     string public post_data;
8
9     function postString (string memory data) public {
10         post_data = data;
11     }
12
13     function getString () public view returns (string memory) {
14         return post_data;
15     }
16 }
```

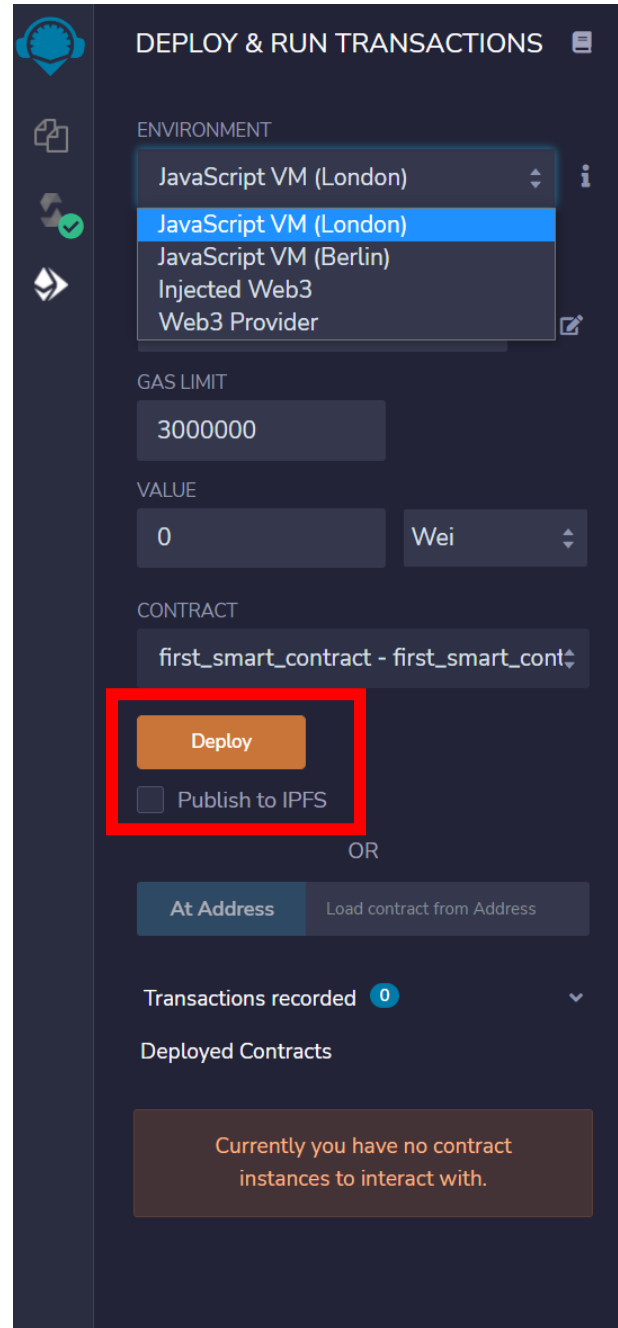
Remix 활용



The screenshot shows the 'SOLIDITY COMPILER' panel in the Remix IDE. The interface is dark-themed. On the left, there are icons for file explorer, compiler, and deployment. The main area contains the following settings:

- COMPILER**: 0.8.7+commit.e28d00a7
- ☐ Include nightly builds
- LANGUAGE**: Solidity
- EVM VERSION**: compiler default
- COMPILER CONFIGURATION**:
 - ☒ Auto compile
 - ☐ Enable optimization (200)
 - ☐ Hide warnings

A large blue button labeled 'Compile' is visible, with 'first_smart_contract.sol' below it. At the bottom, there is a 'CONTRACT' section with a dropdown menu showing 'first_smart_contract (first_smart_contr...' and two buttons: 'Publish on Ipfs' and 'Compilation Details'. At the very bottom, there are links for 'ABI' and 'Bytecode'.



The screenshot shows the 'DEPLOY & RUN TRANSACTIONS' panel in the Remix IDE. The interface is dark-themed. On the left, there are icons for file explorer, compiler, and deployment. The main area contains the following settings:

- ENVIRONMENT**: A dropdown menu is open, showing options: JavaScript VM (London), JavaScript VM (London) (highlighted), JavaScript VM (Berlin), Injected Web3, and Web3 Provider.
- GAS LIMIT**: 3000000
- VALUE**: 0 Wei
- CONTRACT**: first_smart_contract - first_smart_contr...
- A red box highlights the **Deploy** button and the ☐ Publish to IPFS checkbox.
- OR**: A section with a button 'At Address' and a link 'Load contract from Address'.
- Transactions recorded**: 0
- Deployed Contracts**: A message box states: 'Currently you have no contract instances to interact with.'

Remix 활용

The screenshot displays the Remix IDE interface. On the left sidebar, the 'DEPLOY & RUN TRANSACTIONS' panel is active. It shows the following settings:

- ENVIRONMENT: JavaScript VM (London)
- ACCOUNT: 0x5B3...eddC4 (99.9999999%)
- GAS LIMIT: 3000000
- VALUE: 0 Wei
- CONTRACT: first_smart_contract - first_smart_cont

The 'Deploy' button is highlighted. Below it, the 'At Address' tab is selected, showing a list of transactions. The bottom panel displays a successful transaction log:

```
[vm] from: 0x5B3...eddC4 to: first_smart_contract.(constructor) value: 0 wei data: 0x608...70033 logs: 0 hash: 0x9b2...c3413
```

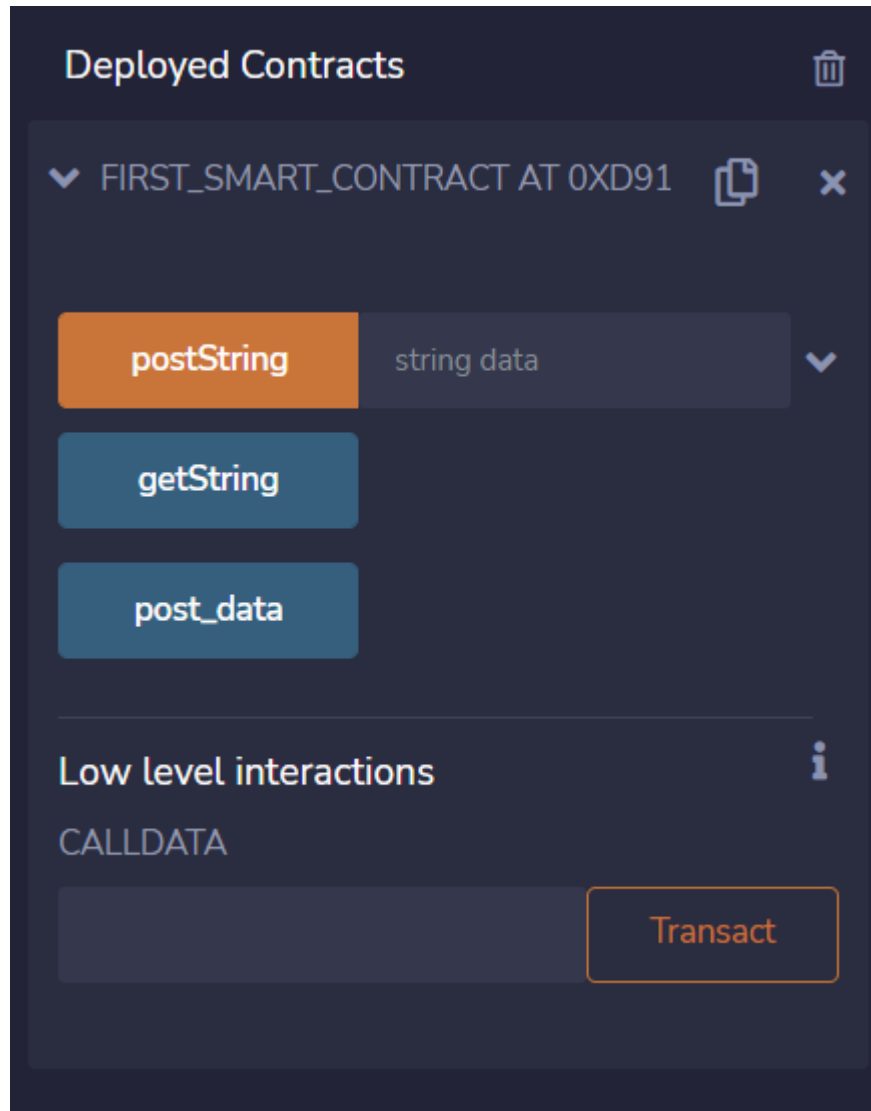
The transaction log is highlighted with a red box. The main editor area shows the Solidity code for the 'first_smart_contract'.

```
// 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

Deployed Contracts

▼ FIRST_SMART_CONTRACT AT 0XD91

postString hello world

getString

post_data

Low level interactions

CALLDATA

Transact

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

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



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

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

Use Ethereum ▾

Learn ▾

Developers ▾

Enterprise ▾

Community ▾

Search

🌙 🌐 Languages

Home Docs **Tutorials** Learn by coding Set up local environment

Overview

Foundational topics ▾

Intro to Ethereum

Intro to Ether

Intro to dapps

Web2 vs Web3

Accounts

Transactions

Blocks

Ethereum virtual machine (EVM)

Gas

Nodes and clients

Networks

Consensus mechanisms

Ethereum stack ▾

Intro to the stack

Smart contracts

Development networks

Development frameworks

Ethereum client APIs

Data and analytics

Storage

Integrated Development Environments (IDEs)

Programming languages

Advanced ▾

Standards

ERC-20 TOKEN STANDARD

Last edit: [@wackerow](#) , December 4, 2021

See contributors

Edit page

Zen Mode

ON THIS PAGE

Introduction

Prerequisites

Body

Examples

Further reading

INTRODUCTION

What is a Token?

Tokens can represent virtually anything in Ethereum:

- reputation points in an online platform
- skills of a character in a game
- lottery tickets
- financial assets like a share in a company
- a fiat currency like USD
- an ounce of gold
- and more...

Such a powerful feature of Ethereum must be handled by a robust standard, right? That's exactly where the ERC-20 plays its role! This standard allows developers to build token applications that are interoperable with other products and services.

What is ERC-20?

The ERC-20 introduces a standard for Fungible Tokens, in other words, they have a property that makes each Token be exactly the same (in type and value) of another Token. For example, an ERC-20 Token acts just like the ETH, meaning that 1 Token is and will always be equal to all the other Tokens.

PREREQUISITES

- [Accounts](#)

Methods

Show less Copy

```
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)
10
```

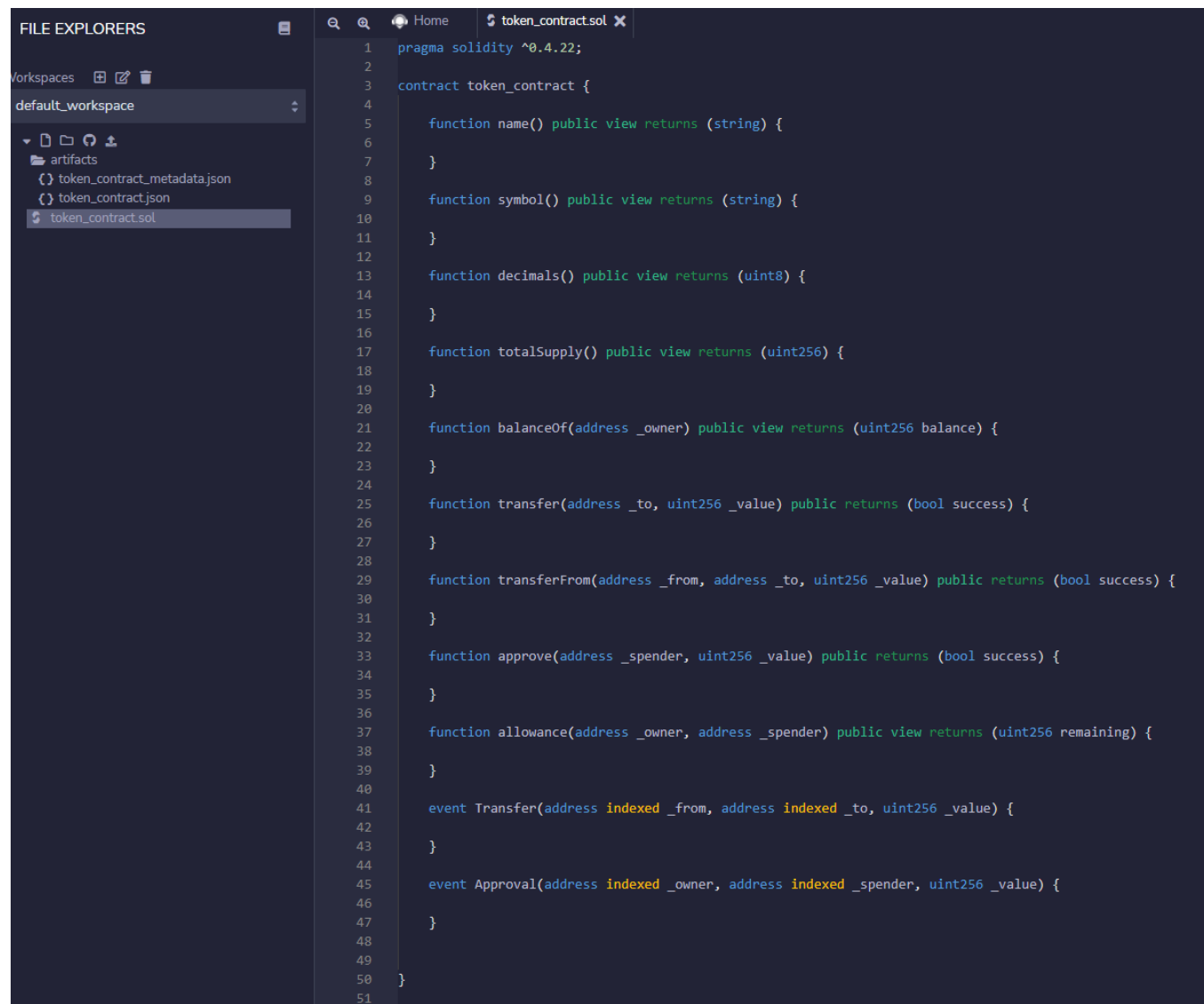
Events

Copy

```
1 event Transfer(address indexed _from, address indexed _to, uint256
  _value)
2 event Approval(address indexed _owner, address indexed _spender, uint256
  _value)
3
```

26


토큰 발행 실습



The image shows a screenshot of a Solidity IDE. On the left, the 'FILE EXPLORERS' panel displays the project structure under 'default_workspace', including 'artifacts', 'token_contract_metadata.json', 'token_contract.json', and 'token_contract.sol'. The main editor area shows the code for 'token_contract.sol' with the following content:

```
1 pragma solidity ^0.4.22;
2
3 contract token_contract {
4
5     function name() public view returns (string) {
6
7     }
8
9     function symbol() public view returns (string) {
10
11    }
12
13    function decimals() public view returns (uint8) {
14
15    }
16
17    function totalSupply() public view returns (uint256) {
18
19    }
20
21    function balanceOf(address _owner) public view returns (uint256 balance) {
22
23    }
24
25    function transfer(address _to, uint256 _value) public returns (bool success) {
26
27    }
28
29    function transferFrom(address _from, address _to, uint256 _value) public returns (bool success) {
30
31    }
32
33    function approve(address _spender, uint256 _value) public returns (bool success) {
34
35    }
36
37    function allowance(address _owner, address _spender) public view returns (uint256 remaining) {
38
39    }
40
41    event Transfer(address indexed _from, address indexed _to, uint256 _value) {
42
43    }
44
45    event Approval(address indexed _owner, address indexed _spender, uint256 _value) {
46
47    }
48
49 }
50
51
```

<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 1

[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 ▾

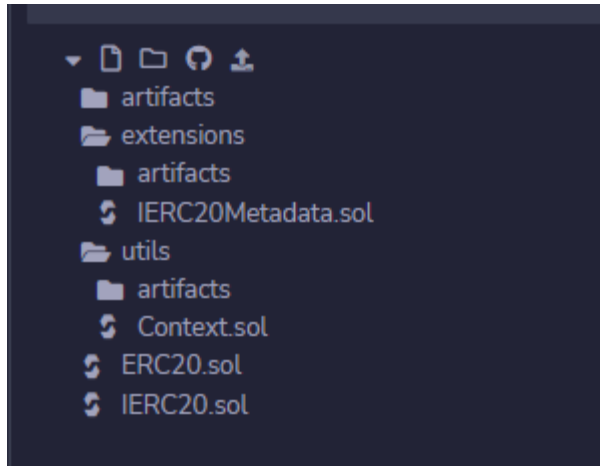
[openzeppelin-contracts](#) / [contracts](#) / [token](#) / [ERC20](#) / [extensions](#) / [IERC20Metadata.sol](#)



master ▾

[openzeppelin-contracts](#) / [contracts](#) / [utils](#) / [Context.sol](#)

토큰 발행 실습



```
ERC20.sol x 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 (99.99999999%)

GAS LIMIT

3000000

VALUE

0 Wei

CONTRACT

ERC20 - ERC20.sol

string name_, string symbol_

☐ Publish to IPFS

OR

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 (99.99999999%)

GAS LIMIT

3000000

VALUE

0 Wei

CONTRACT

ERC20 - ERC20.sol

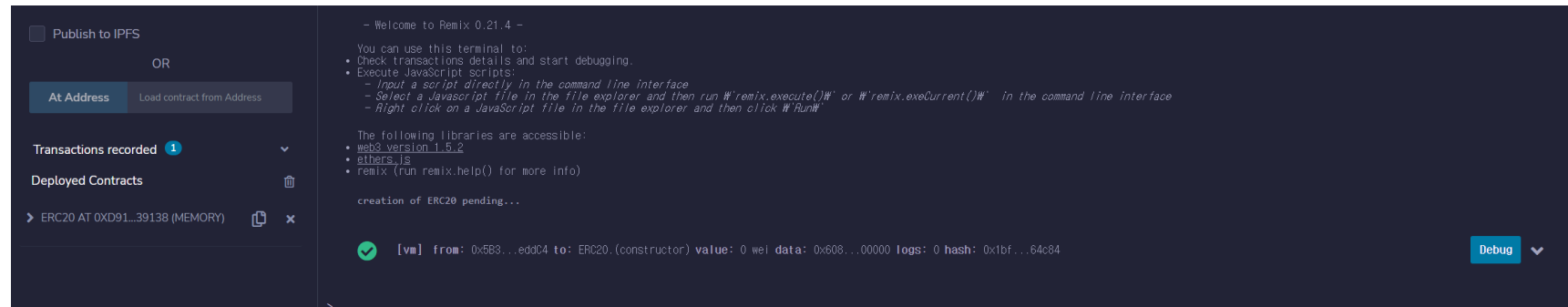
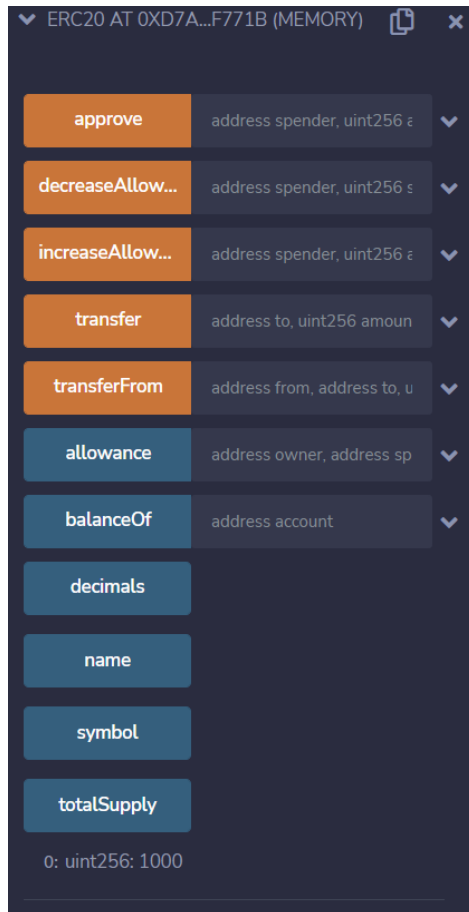
DEPLOY

NAME_: st

SYMBOL_: st

MINT_: 1000

토큰 발행 실습



토콘 발행 실습

베수 실행

MINGW64:/e/besu_privateNetwork/besu_network/node1

```
1H60L3dw7N03Cd1-dbnRwn2F, nodeid=0x87e53fc9ba07935464950dd7b2e54b1f1edast
e33d5a4c463daf85cb96dc85fee31c247c0862d58bea0c7eaeedc, udpAddress=Optional[127.0.0.1:30304], tcpAddress=Optional[127.0.0.1:30304], asBase64=3e4QF0m3XW-38V
P5tYudlCQ14ecExjPAUTyBxkT1n6p9sb1AA1PAH0NjRR84t-9nJlPhLRdyP_c1ptPV9C9ce80ig2V0a
WfGHd5eK1Agm1kgN0ghu8AAAGCzVjvCD11Mmx0Q9PLB83m-MWkxGPN-X4LL1tyF_uWCJKAaC1
VhD9581N0Y3CCmD8R0wgnZ, nodeid=0x8385194f780983f8027ecf6a271e6f844e08cec
4861cf373994aa16555c3b, customFields={tcp=30304, udp=30304, ip=0x7f000001, eth=1
[0x575278a8, 0x]}, id=v4, secp256k1=0x03fa2c17b79be33d5a4c463daf85cb96dc85fee31
c247c0862d58bea0c7eaeedc}
2022-03-06 12:22:42.661+09:00 | main | INFO | DefaultP2PNetwork | Enode URL eno
de://fa2c17b79be33d5a4c463daf85cb96dc85fee31c247c0862d58bea0c7eaeedc11872275c07
238d51ba983201c0300f6e1ab850bc192ad98f13fce3b5da670127.0.0.1:30304
2022-03-06 12:22:42.663+09:00 | main | INFO | DefaultP2PNetwork | Node address
0x61e71e67841ac08cec4861c3f23994aa16555c3b
2022-03-06 12:22:42.666+09:00 | main | INFO | Defaultsynchronizer | Starting sy
nchronizer
2022-03-06 12:22:42.674+09:00 | main | INFO | FullSyncDownloader | Starting ful
l sync
2022-03-06 12:22:37.686+09:00 | main | INFO | FullSyncTargetManager | No sync t
arget, waiting for peers. Current peers: 0
2022-03-06 12:22:37.941+09:00 | main | INFO | Runner | Ethereum main loop is up
2022-03-06 12:22:42.699+09:00 | EthScheduler-Timer-0 | INFO | FullSyncTargetMa
nager | No sync target, waiting for peers. Current peers: 0
2022-03-06 12:22:43.216+09:00 | nioEventLoopGroup-3-1 | INFO | FullSyncTargetMa
nager | No sync target, waiting for peers. Current peers: 1
2022-03-06 12:22:47.826+09:00 | nioEventLoopGroup-3-1 | INFO | SyncTargetManage
r | Found common ancestor with peer Peer 0xfa2c17b79be33d5a4c... at block 850
```

MINGW64:/e/besu_privateNetwork/besu_network/node2

```
e33d5a4c463daf85cb96dc85fee31c247c0862d58bea0c7eaeedc, udpAddress=Optional[127.0.0.1:30304], tcpAddress=Optional[127.0.0.1:30304], asBase64=3e4QF0m3XW-38V
P5tYudlCQ14ecExjPAUTyBxkT1n6p9sb1AA1PAH0NjRR84t-9nJlPhLRdyP_c1ptPV9C9ce80ig2V0a
WfGHd5eK1Agm1kgN0ghu8AAAGCzVjvCD11Mmx0Q9PLB83m-MWkxGPN-X4LL1tyF_uWCJKAaC1
VhD9581N0Y3CCmD8R0wgnZ, nodeid=0x8385194f780983f8027ecf6a271e6f844e08cec
4861cf373994aa16555c3b, customFields={tcp=30304, udp=30304, ip=0x7f000001, eth=1
[0x575278a8, 0x]}, id=v4, secp256k1=0x03fa2c17b79be33d5a4c463daf85cb96dc85fee31
c247c0862d58bea0c7eaeedc}
2022-03-06 12:22:42.661+09:00 | main | INFO | DefaultP2PNetwork | Enode URL eno
de://fa2c17b79be33d5a4c463daf85cb96dc85fee31c247c0862d58bea0c7eaeedc11872275c07
238d51ba983201c0300f6e1ab850bc192ad98f13fce3b5da670127.0.0.1:30304
2022-03-06 12:22:42.663+09:00 | main | INFO | DefaultP2PNetwork | Node address
0x61e71e67841ac08cec4861c3f23994aa16555c3b
2022-03-06 12:22:42.666+09:00 | main | INFO | Defaultsynchronizer | Starting sy
nchronizer
2022-03-06 12:22:42.674+09:00 | main | INFO | FullSyncDownloader | Starting ful
l sync
2022-03-06 12:22:42.676+09:00 | main | INFO | FullSyncTargetManager | No sync t
arget, waiting for peers. Current peers: 0
2022-03-06 12:22:43.008+09:00 | main | INFO | Runner | Ethereum main loop is up
2022-03-06 12:22:43.215+09:00 | nioEventLoopGroup-3-2 | INFO | FullSyncTargetMa
nager | No sync target, waiting for peers. Current peers: 2
```

MINGW64:/e/besu_privateNetwork/besu_network/node3

```
24b4e495d7e547824b7c0c07d5dc0d3531ae96e26dbb281ef, udpAddress=Optional[127.0.0.1:30305], tcpAddress=Optional[127.0.0.1:30305], asBase64=3e4QF0m3XW-38V
P5tYudlCQ14ecExjPAUTyBxkT1n6p9sb1AA1PAH0NjRR84t-9nJlPhLRdyP_c1ptPV9C9ce80ig2V0a
WfGHd5eK1Agm1kgN0ghu8AAAGCzVjvCD11Mmx0Q9PLB83m-MWkxGPN-X4LL1tyF_uWCJKAaC1
VhD9581N0Y3CCmD8R0wgnZ, nodeid=0x8385194f780983f8027ecf6a271e6f844e08cec
4861cf373994aa16555c3b, customFields={tcp=30305, udp=30305, ip=0x7f000001, eth=1
[0x575278a8, 0x]}, id=v4, secp256k1=0x02fb7862c95802a4be4a95d7e547824b7c9ce0475d
809531ae96e26dbb281ef}
2022-03-06 12:22:47.361+09:00 | main | INFO | DefaultP2PNetwork | Enode URL eno
de://fb7862c95802a4be4a95d7e547824b7c9ce0475d809531ae96e26dbb281efeld93b6f886
9a715b6f2703c5601d068c9f2ef49804d1c4d6dd2c8abb1c083127.0.0.1:30305
2022-03-06 12:22:47.362+09:00 | main | INFO | DefaultP2PNetwork | Node address
x952bae1dd731bc375f784d1990fddcf7e0cf7b38
2022-03-06 12:22:47.367+09:00 | main | INFO | Defaultsynchronizer | Starting sy
nchronizer
2022-03-06 12:22:47.370+09:00 | main | INFO | FullSyncDownloader | Starting ful
l sync
2022-03-06 12:22:47.371+09:00 | main | INFO | FullSyncTargetManager | No sync t
arget, waiting for peers. Current peers: 0
2022-03-06 12:22:47.687+09:00 | main | INFO | Runner | Ethereum main loop is up
2022-03-06 12:22:47.790+09:00 | nioEventLoopGroup-3-4 | INFO | FullSyncTargetMa
nager | No sync target, waiting for peers. Current peers: 3
```

MINGW64:/e/besu_privateNetwork/besu_network/node4

```
1 schedule created with milestones: [MuirGlacier: 0]
2022-03-06 12:22:49.568+09:00 | main | INFO | RunnerBuilder | Detecting NAT ser
vice
2022-03-06 12:22:49.702+09:00 | main | INFO | Runner | Starting external servic
es
2022-03-06 12:22:49.703+09:00 | main | INFO | WebsocketService | Starting Webso
cket service on 127.0.0.1:8548
2022-03-06 12:22:50.468+09:00 | vert.x-eventloop-thread-1 | INFO | WebsocketSer
vice | Websocket service started and listening on 127.0.0.1:8548
2022-03-06 12:22:50.470+09:00 | main | INFO | AutoTransactionLogBloomCachingSer
vice | Starting auto transaction log bloom caching service
2022-03-06 12:22:50.472+09:00 | main | INFO | LogBloomCacheMetadata | Lookup ca
che metadata file in data directory: E:\besu_privateNetwork\besu_network\node4\d
ata\caches
2022-03-06 12:22:50.484+09:00 | main | INFO | Runner | Starting Ethereum main l
oop
2022-03-06 12:22:50.484+09:00 | main | INFO | NatService | No NAT environment d
etected so no service could be started
2022-03-06 12:22:50.485+09:00 | main | INFO | NetworkRunner | Starting Network
2022-03-06 12:22:50.491+09:00 | nioEventLoopGroup-2-1 | INFO | RlpAgent | P2P
Rlp agent started and listening on /0x0300000000:30306
2022-03-06 12:22:50.492+09:00 | main | INFO | PeerDiscoveryAgent | Starting pee
r discovery agent on host=0.0.0.0, port=30306
```

MINGW64:/e/besu_privateNetwork/besu_network/node1

```
ntrollerBuilder | Produced #855 / 0 tx / 0 pending / 0 (0.0%) gas / (0xe1370b6dc
29011cd789b99c9be5bc943bbfb6e3415ff3c5b278571dde7751434)
2022-03-06 12:22:59.251+09:00 | EthScheduler-Workers-0 | INFO | PersistBlockTas
k | Imported #856 / 0 tx / 0 om / 0 (0.0%) gas / (0x5ae77f3a97ac83be948e6b9b676e
57101fc89d6f454123ddb6b1c2ff0a53bf37) in 0.011s. Peers: 3
2022-03-06 12:22:59.253+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #856 / 0 tx / 0 pending / 0 (0.0%) gas / (0x5ae77f3a9
7ac83be948e6b9b676e57101fc89d6f454123ddb6b1c2ff0a53bf37)
2022-03-06 12:23:01.263+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a51bdf1f7c349de5be59c921bbf56e6adc7041ba2b013)
2022-03-06 12:23:01.255+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a51bdf1f7c349de5be59c921bbf56e6adc7041ba2b013)
2022-03-06 12:23:03.124+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #858 / 0 tx / 0 pending / 0 (0.0%) gas / (0x772f8c371
914787b1309d2a31055f974f37c0419604bf3cd2c062e919e1ad84d)
2022-03-06 12:23:05.141+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Produced #859 / 0 tx / 0 pending / 0 (0.0%) gas / (0xca7a8d320
1b71daa414314b10414f25e07ee52542febe90d1612982a74488b1)
2022-03-06 12:23:07.247+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #860 / 0 tx / 0 pending / 0 (0.0%) gas / (0xb823b657d
c2d5c8aec2381a0a65b91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.010s. Peers: 3
```

MINGW64:/e/besu_privateNetwork/besu_network/node2

```
k | Imported #856 / 0 tx / 0 om / 0 (0.0%) gas / (0x5ae77f3a97ac83be948e6b9b676e
57101fc89d6f454123ddb6b1c2ff0a53bf37) in 0.026s. Peers: 4
2022-03-06 12:22:59.234+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #856 / 0 tx / 0 pending / 0 (0.0%) gas / (0x5ae77f3a9
7ac83be948e6b9b676e57101fc89d6f454123ddb6b1c2ff0a53bf37)
2022-03-06 12:23:01.263+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a51bdf1f7c349de5be59c921bbf56e6adc7041ba2b013)
2022-03-06 12:23:03.129+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Produced #858 / 0 tx / 0 pending / 0 (0.0%) gas / (0x772f8c371
914787b1309d2a31055f974f37c0419604bf3cd2c062e919e1ad84d)
2022-03-06 12:23:05.149+09:00 | EthScheduler-Workers-2 | INFO | PersistBlockTas
k | Imported #859 / 0 tx / 0 om / 0 (0.0%) gas / (0xca7a8d3201b71daa414314b1041
4f25e07ee52542febe90d1612982a74488b1) in 0.005s. Peers: 4
2022-03-06 12:23:05.149+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #859 / 0 tx / 0 pending / 0 (0.0%) gas / (0xca7a8d320
1b71daa414314b10414f25e07ee52542febe90d1612982a74488b1)
2022-03-06 12:23:07.234+09:00 | EthScheduler-Workers-0 | INFO | PersistBlockTas
k | Imported #860 / 0 tx / 0 om / 0 (0.0%) gas / (0xb823b657dcd25c8aec2381a0a65b
91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.010s. Peers: 3
```

MINGW64:/e/besu_privateNetwork/besu_network/node3

```
ntrollerBuilder | Imported #854 / 0 tx / 0 pending / 0 (0.0%) gas / (0x4ee72cfcb
4b677a2f228a65c262b9bbdbf9454781e396cafa4d345d2cbb6eac533)
2022-03-06 12:22:57.253+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #855 / 0 tx / 0 pending / 0 (0.0%) gas / (0xe1370b6dc
29011cd789b99c9be5bc943bbfb6e3415ff3c5b278571dde7751434)
2022-03-06 12:22:59.196+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Produced #856 / 0 tx / 0 pending / 0 (0.0%) gas / (0x5ae77f3a9
7ac83be948e6b9b676e57101fc89d6f454123ddb6b1c2ff0a53bf37)
2022-03-06 12:23:01.257+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a51bdf1f7c349de5be59c921bbf56e6adc7041ba2b013)
2022-03-06 12:23:03.133+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #858 / 0 tx / 0 pending / 0 (0.0%) gas / (0x772f8c371
914787b1309d2a31055f974f37c0419604bf3cd2c062e919e1ad84d)
2022-03-06 12:23:05.146+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #859 / 0 tx / 0 pending / 0 (0.0%) gas / (0xca7a8d320
1b71daa414314b10414f25e07ee52542febe90d1612982a74488b1)
2022-03-06 12:23:05.155+09:00 | EthScheduler-Workers-0 | INFO | PersistBlockTas
k | Imported #854 / 0 tx / 0 om / 0 (0.0%) gas / (0xe1370b6dc29011cd789b99c9be5b
91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.000s. Peers: 4
2022-03-06 12:23:07.221+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Produced #860 / 0 tx / 0 pending / 0 (0.0%) gas / (0xb823b657d
c2d5c8aec2381a0a65b91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.010s. Peers: 3
```


MINGW64:/e/besu_privateNetwork/besu_network/node4

```
k | Imported #855 / 0 tx / 0 om / 0 (0.0%) gas / (0xe1370b6dc29011cd789b99c9be5b
91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.000s. Peers: 4
2022-03-06 12:22:57.242+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #855 / 0 tx / 0 pending / 0 (0.0%) gas / (0xe1370b6dc
29011cd789b99c9be5bc943bbfb6e3415ff3c5b278571dde7751434)
2022-03-06 12:22:59.221+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #856 / 0 tx / 0 pending / 0 (0.0%) gas / (0x5ae77f3a9
7ac83be948e6b9b676e57101fc89d6f454123ddb6b1c2ff0a53bf37)
2022-03-06 12:23:01.244+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Produced #857 / 0 tx / 0 pending / 0 (0.0%) gas / (0x7206b5357
a36037c613a51bdf1f7c349de5be59c921bbf56e6adc7041ba2b013)
2022-03-06 12:23:03.133+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #858 / 0 tx / 0 pending / 0 (0.0%) gas / (0x772f8c371
914787b1309d2a31055f974f37c0419604bf3cd2c062e919e1ad84d)
2022-03-06 12:23:03.133+09:00 | EthScheduler-Workers-1 | INFO | PersistBlockTas
k | Imported #858 / 0 tx / 0 om / 0 (0.0%) gas / (0x772f8c371914787b1309d2a31055
f974f37c0419604bf3cd2c062e919e1ad84d) in 0.005s. Peers: 4
2022-03-06 12:23:05.135+09:00 | BftProcessorExecutor-IBFT-0 | INFO | IbfBtBesuCo
ntrollerBuilder | Imported #859 / 0 tx / 0 pending / 0 (0.0%) gas / (0xb823b657d
c2d5c8aec2381a0a65b91c4e000d46f87a53fcd90096dbf24b3ad6) in 0.010s. Peers: 3
```


34



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


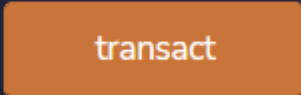
ERC20 - ERC20.sol 

DEPLOY 

NAME_: jw

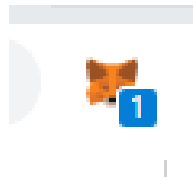
SYMBOL_: jw

MINT_: 9000000000000000000

토큰 발행 실습

creation of ERC20 pending...



test_network

Account 15 → 새 계약

<https://remix.ethereum.org>

계약 배포

세부 정보 데이터

편집

예상 가스 요금 ⓘ 0 0 ETH
제한 사이트 최대 요금 0 ETH

합계 0 0 ETH
금액 + 가스 요금 최대 금액: 0 ETH

거부 확인

Deployed Contracts

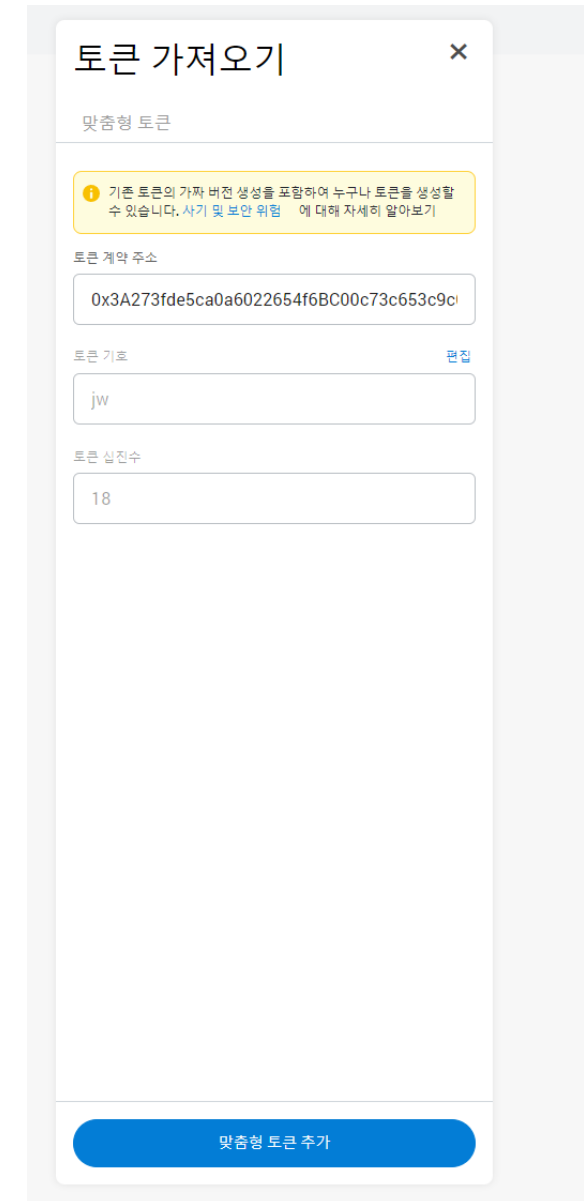
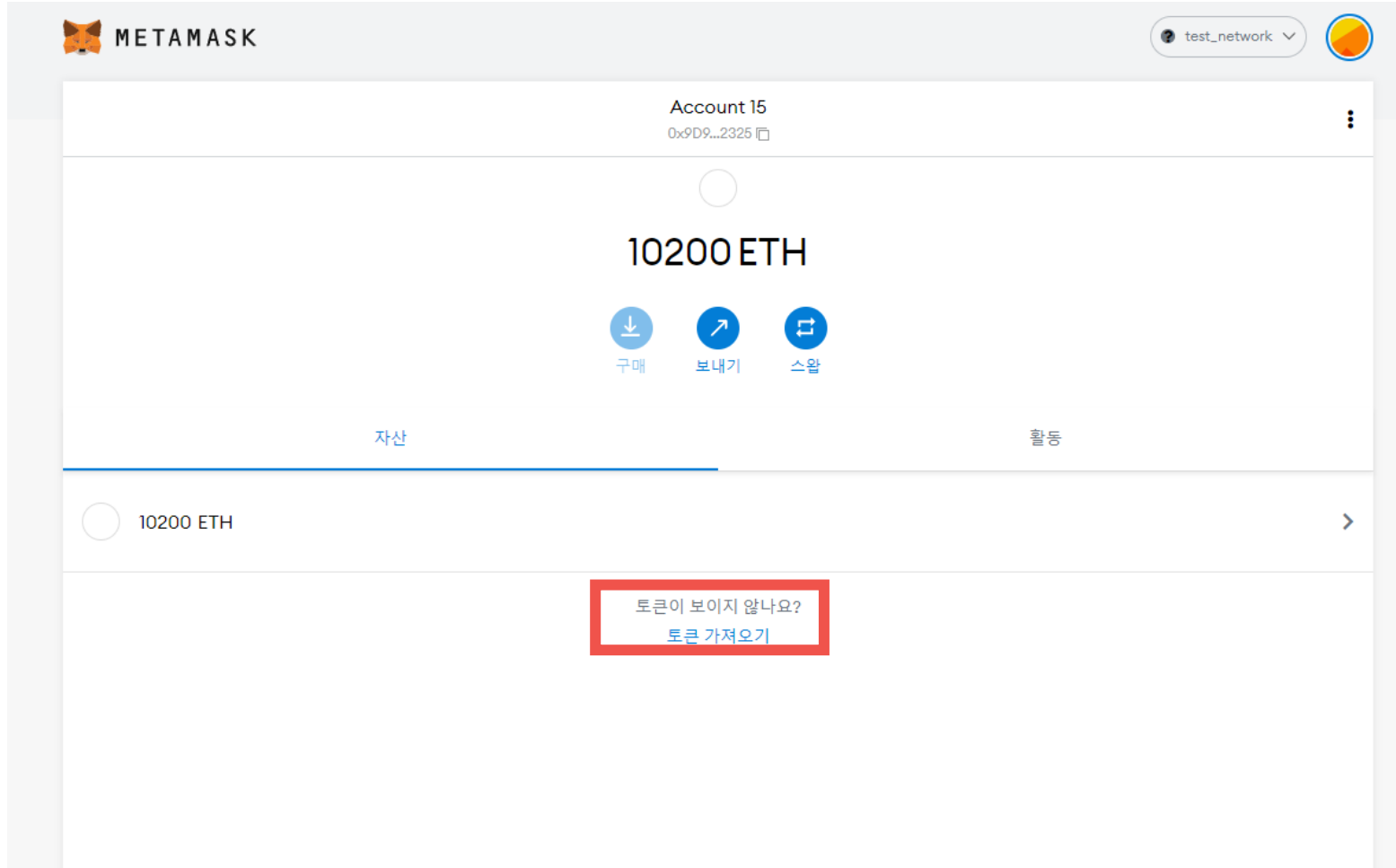
ERC20 AT 0X3A2...C0CFD (BLOCK-H) [copy] [x]

approve	address spender, uint256 z	▼
decreaseAllow...	address spender, uint256 s	▼
increaseAllow...	address spender, uint256 z	▼
transfer	address to, uint256 amoun	▼
transferFrom	address from, address to, u	▼
allowance	address owner, address sp	▼
balanceOf	address account	▼
decimals		
name		
symbol		
totalSupply		

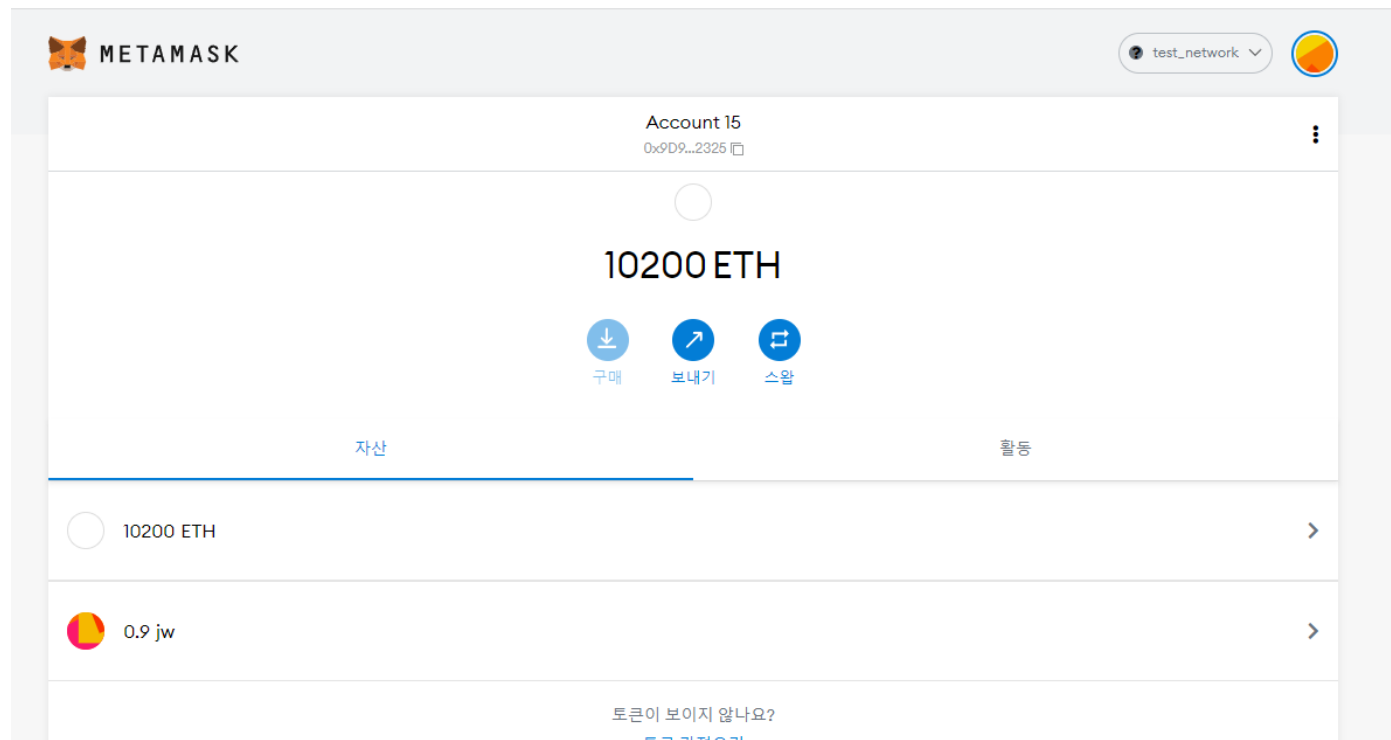
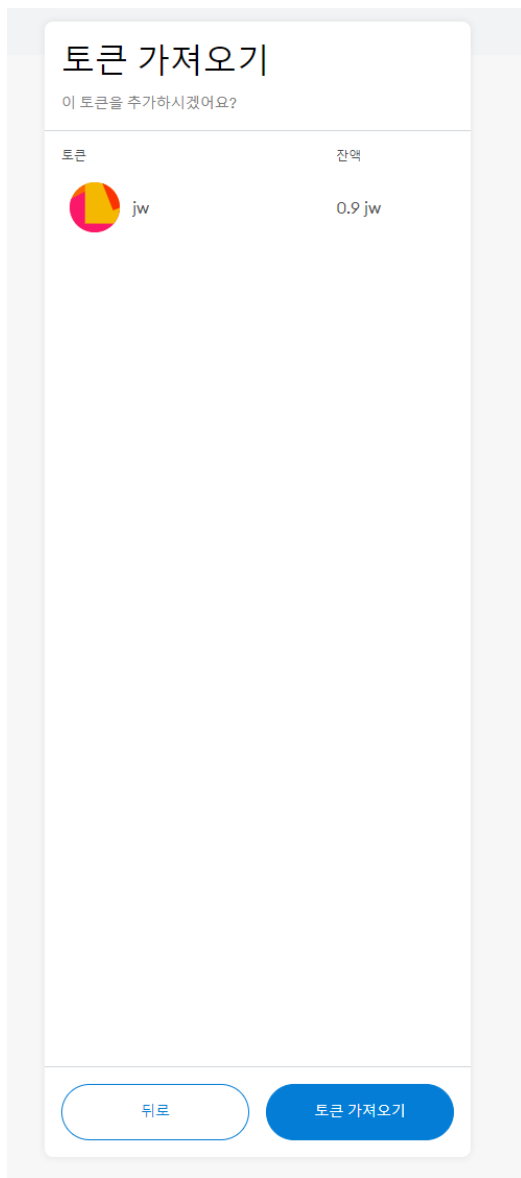
0: uint256: 9000000000000000000

Low level interactions ⓘ
CALLDATA

토큰 발행 실습



토큰 발행 실습



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



The screenshot shows the Atom text editor with a file named `package.json` open. The file path in the title bar is `E:\besu_privateNetwork\besu_wallet`. The left sidebar shows the project structure with a folder named `besu_wallet` containing the `package.json` file. The main editor area displays the following JSON content:

```
1 {
2   "name": "besu_wallet",
3   "version": "1.0.0",
4   "description": "",
5   "main": "index.js",
6   "scripts": {
7     "test": "echo \"Error: no test specified\" && exit 1"
8   },
9   "author": "",
10  "license": "ISC"
11 }
12
```

npm install express npm install web3

```
system888@DESKTOP-QM35NPN 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-QM35NPN 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
```

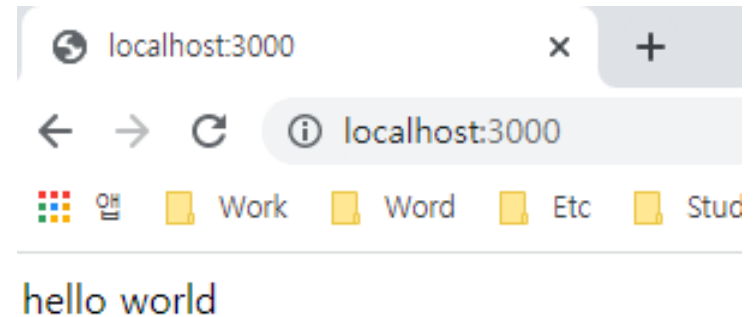
```
package.json
package-lock.json

1  {
2    "name": "besu_wallet",
3    "version": "1.0.0",
4    "description": "",
5    "main": "index.js",
6    "scripts": {
7      "test": "echo \"Error: no test specified\" && exit 1"
8    },
9    "author": "",
10   "license": "ISC",
11   "dependencies": {
12     "express": "^4.17.3",
13     "web3": "^1.7.1"
14   }
15 }
```

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
```



Html 페이지 만들기

```
package.json x
1 {
2   "name": "besu_wallet",
3   "version": "1.0.0",
4   "description": "",
5   "main": "index.js",
6   "scripts": {
7     "test": "echo \"Error: no test specified\" && exit 1"
8   },
9   "author": "",
10  "license": "ISC",
11  "dependencies": {
12    "express": "^4.17.3",
13    "web3": "^1.7.1",
14    "body-parser": "^1.19.0"
15  }
16 }
```

```
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
```

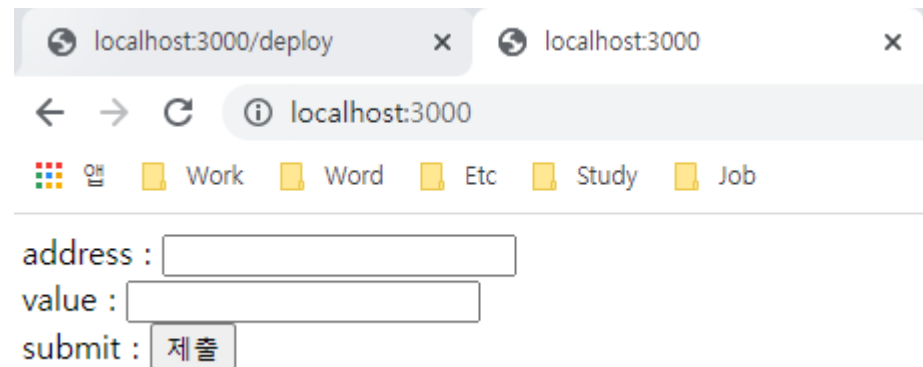
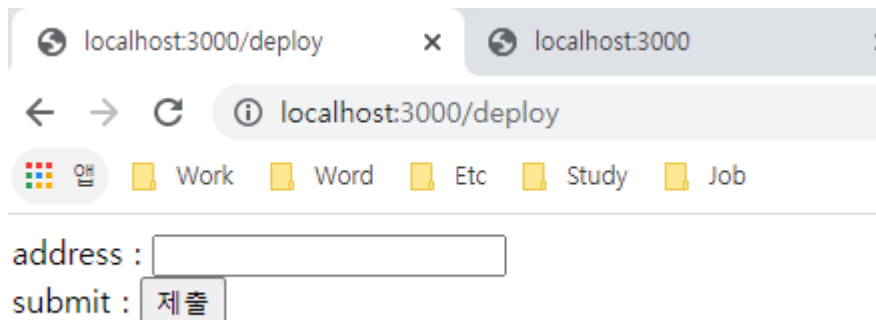
Html 페이지 만들기

```
1 var express = require('express');
2 var app = express();
3 var bodyParser = require('body-parser');
4
5 app.use(bodyParser.json())
6 app.use(bodyParser.urlencoded({ extended: true}));
7
8
9 app.get('/', function(req, res){
10   res.sendFile(__dirname+ "/index.html")
11 })
12
13 app.get('/deploy', function(req, res){
14   res.sendFile(__dirname+ "/deploy.html")
15 })
16
17 var server = app.listen(3000, function(){
18   console.log("server is working now")
19 })
```


```
server.js  deploy.html  index.html
1 <form action="post" method="post">
2   address : <input type="text" name="address" /><br />
3   submit : <input type="submit" />
4 </form>
```

```
server.js  x  deploy.html  index.html
1 <form action="post" method="post">
2   address : <input type="text" name="address" /><br />
3   value : <input type="text" name="value" /> <br />
4   submit : <input type="submit" />
5 </form>
```

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

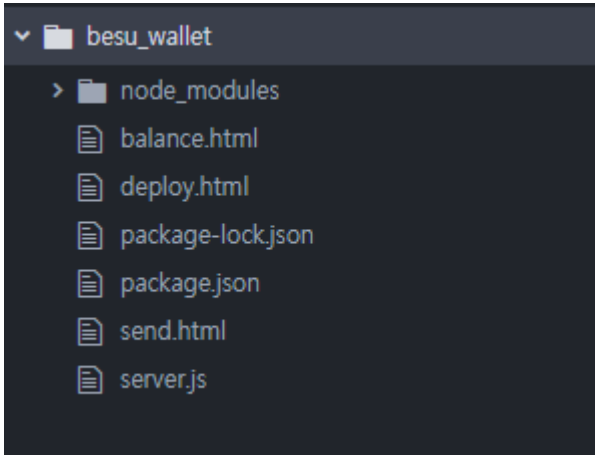
▶ DEVDOC

▶ USERDOC

▶ RUNTIME BYTECODE

▶ ASSEMBLY

파일 및 package.json 내용



```
1  {
2    "name": "besu_wallet",
3    "version": "1.0.0",
4    "description": "",
5    "main": "index.js",
6    "scripts": {
7      "test": "echo \"Error: no test specified\" && exit 1"
8    },
9    "author": "",
10   "license": "ISC",
11   "dependencies": {
12     "express": "^4.17.3",
13     "web3": "^1.7.1",
14     "body-parser": "^1.19.0",
15     "ethereumjs-tx": "^1.3.7"
16   }
17 }
```

Html 파일

```
deploy.html x
1 <form action="/deploy" method="post">
2   token_name: <input type="text" name="tn" /><br />
3   token_symbol: <input type="text" name="ts" /><br />
4   total_supply: <input type="text" name="supply" /><br />
5   submit : <input type="submit" />
6 </form>
```

```
send.html x
1 <form action="/send" method="post">
2   address : <input type="text" name="address" /><br />
3   value : <input type="text" name="value" /> <br />
4   submit : <input type="submit" />
5 </form>
```

```
balance.html x
1 <form action="/balance" method="post">
2   address : <input type="text" name="address" /><br />
3   submit : <input type="submit" />
4 </form>
```

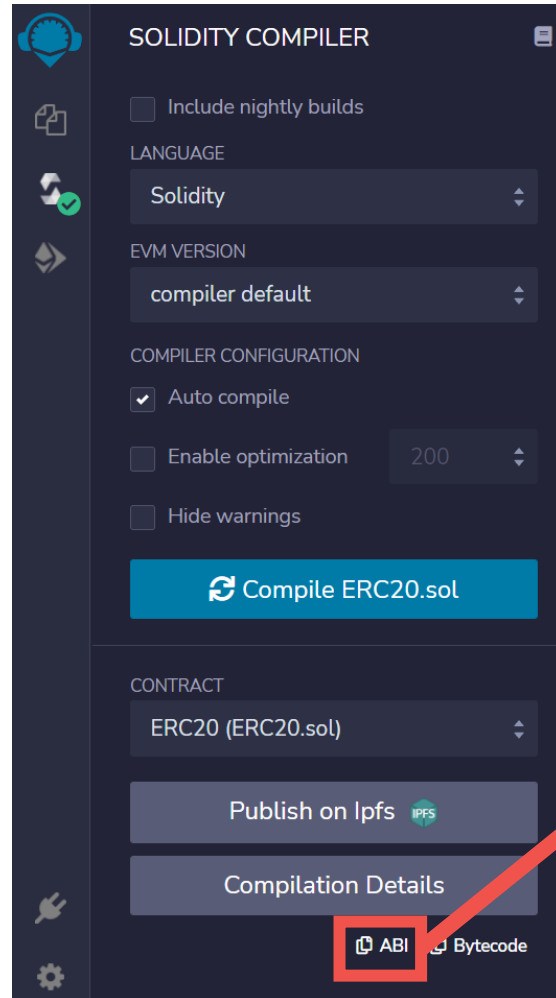
Server.js 파일

```
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

Server.js 파일



복사

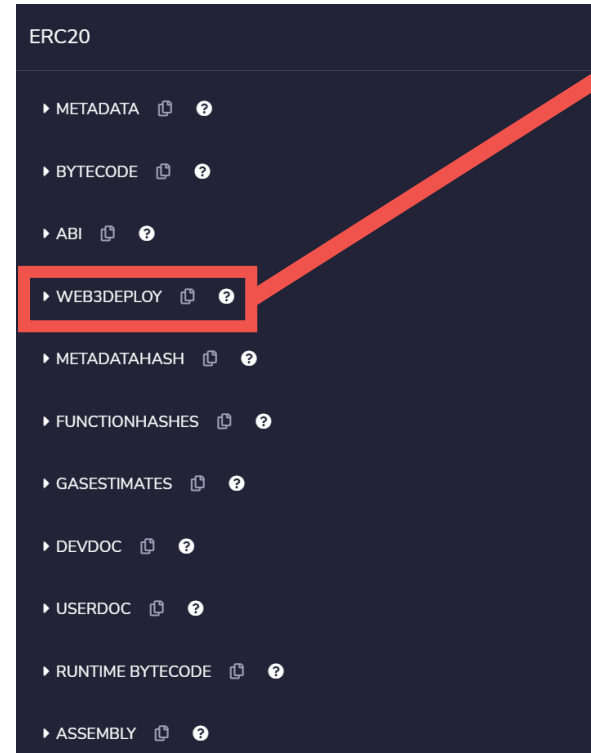
```
13 var ABI = [
14 {
15   "inputs": [
16     {
17       "internalType": "string",
18       "name": "name_",
19       "type": "string"
20     },
21     {
22       "internalType": "string",
23       "name": "symbol_",
24       "type": "string"
25     },
26     {
27       "internalType": "uint256",
28       "name": "mint_",
29       "type": "uint256"
30     }
31   ],
32   "stateMutability": "nonpayable",
33   "type": "constructor"
34 },
35 {
36   "anonymous": false,
37   "inputs": [
38     {
39       "indexed": true,
40       "internalType": "address",
41       "name": "owner",
42       "type": "address"
43     },
44     {
45       "indexed": true,
46       "internalType": "address",
47       "name": "spender",
48       "type": "address"
49     }
50   ]
51 }
52 ]
```

지갑 만들기 실습

Server.js 파일

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

```
318 v 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:
    '0x60806040523480156200001157600080fd5b506040516200194
fd5b6200010b60008383620001fd60201b60201c565b8060026000
36200020260201b60201c565b5050565b505050565b5050565b8
565b7f4e487b7100000000000000000000000000000000000000
d620003e7846200036a565b6200034b565b9050828152602081018
0162000421565b935050602084015167fffffffffffffffff811115
0000600052601160045260246000fd5b6000620005e8826200045
565b5b50919050565b61126880620006db6000396000f3fe608060
d565b610308565b6040516100f39190610c38565b6040518091039
9190610b22565b60405180910390f35b6102006004803603810190
16102fe565b820191906000526020600020905b815481529060010
fffffffffffffffffffffffffffffffffffffffff1681526020019081526020
00000000000000000081526004016104d390610ecc565b604051809
fffffffffffffffffffffffffffffffff168373ffffffffffffffffffffffff
fffffffffffffffffffffffff16815260200190815260200160002
6107f857818110156107ea576040517f08c379a000000000000000
ffff1614156108de576040517f08c379a000000000000000000000
fffffffffffffffffffffffffffffffff168152602001908152602001
00081519050919050565b600082825260208201905092915050565
69565b8114610b8f57600080fd5b50565b600081359050610ba181
15050565b60008060060608486031215610c9657610c95610b445
9050565b7f4e487b71000000000000000000000000000000000000
```

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 })
```

Deploy 결과

[illegible]

×

토큰 가져오기

맞춤형 토큰

i

기존 토큰의 가짜 버전 생성을 포함하여 누구나 토큰을 생성할 수 있습니다. [사기 및 보안 위험](#)에 대해 자세히 알아보기

토큰 계약 주소

0x1f8890b3e32E25d5b8eC8d66BB2f0D828Fe9

토큰 기호

tx

토큰 십진수

18

맞춤형 토큰 추가

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     };
383   });
```

```
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

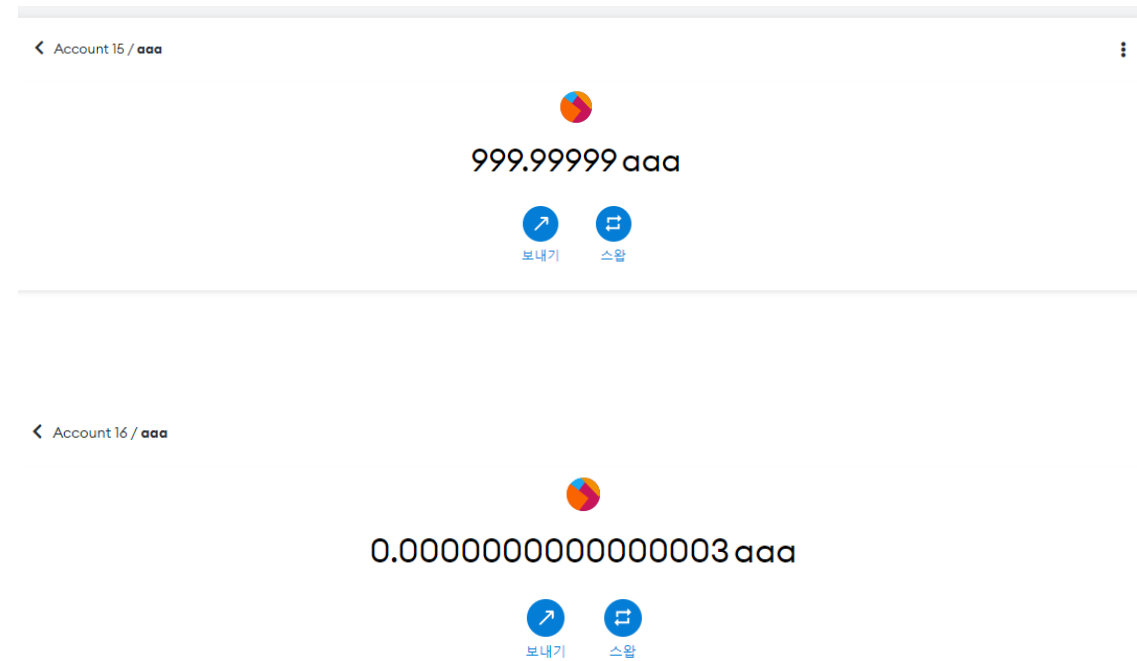
Server.js 파일

```
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 })
```

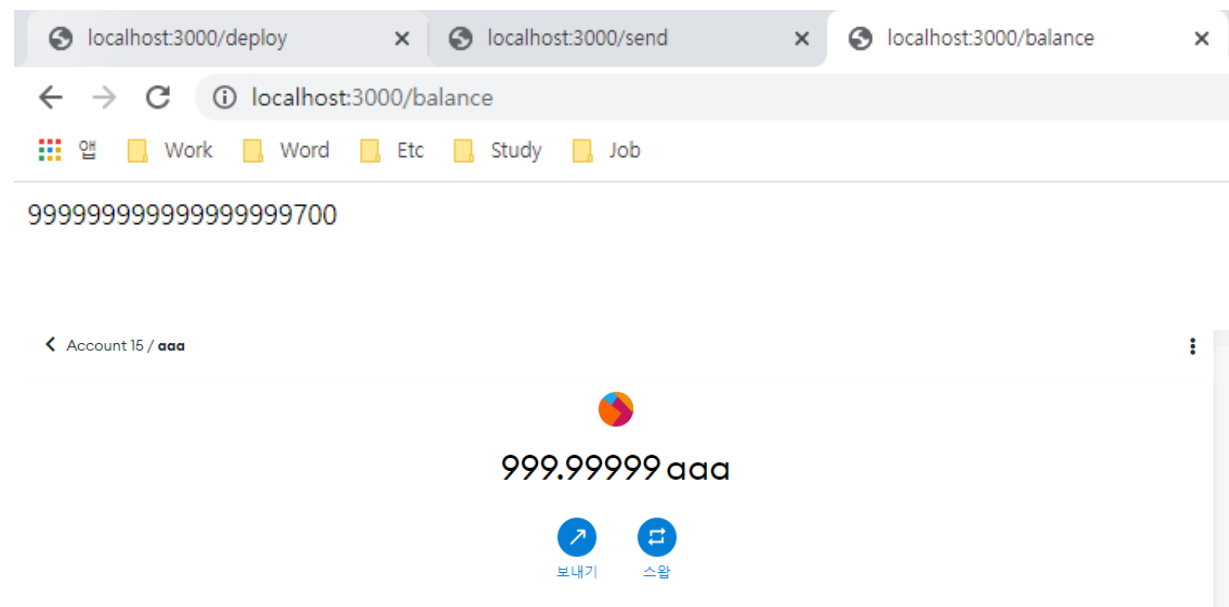
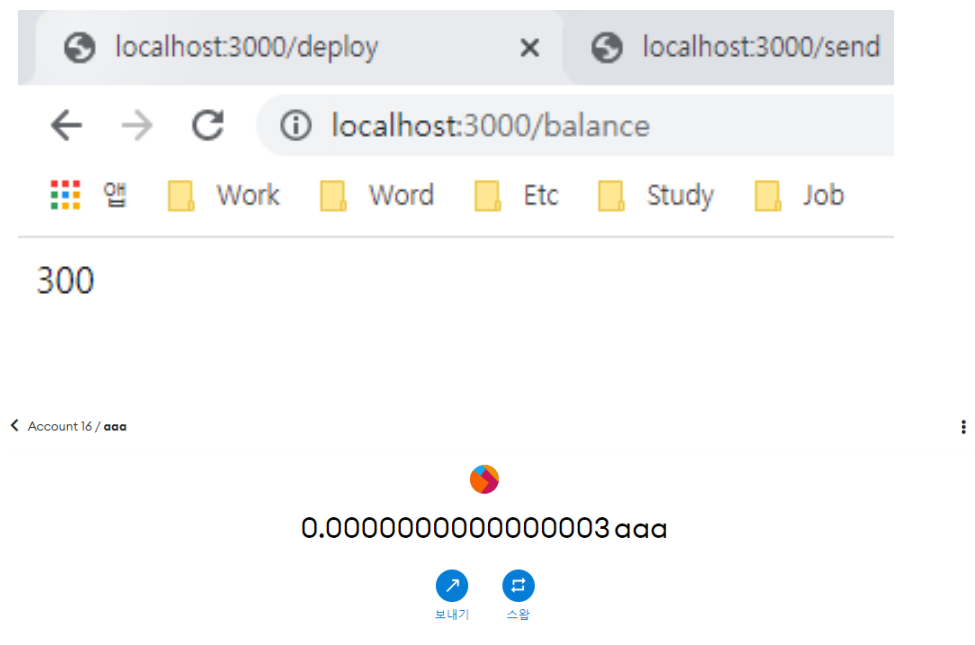
지갑 만들기 실습

[illegible]

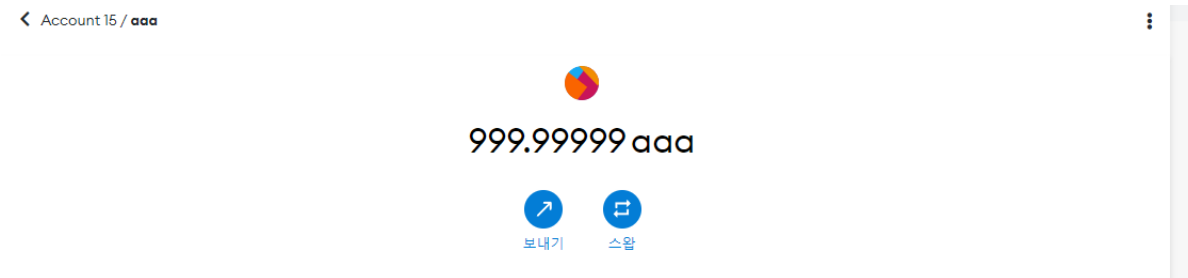
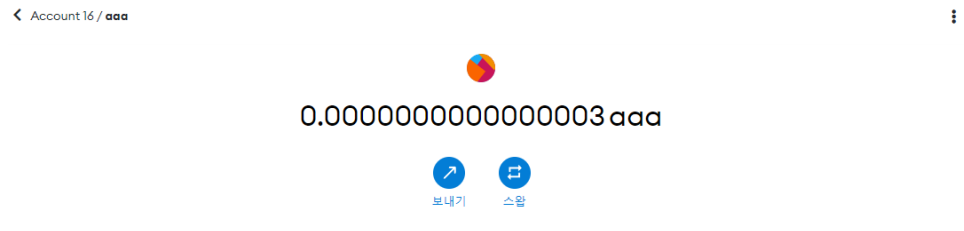
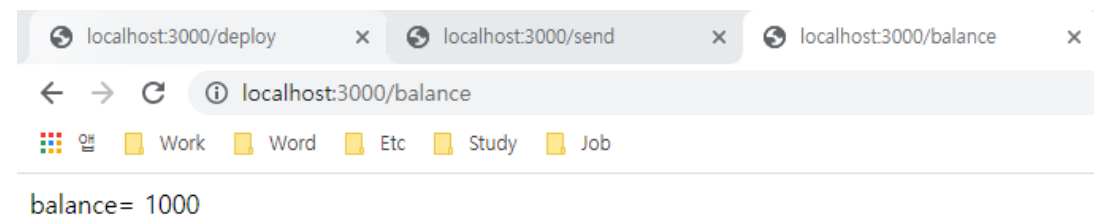
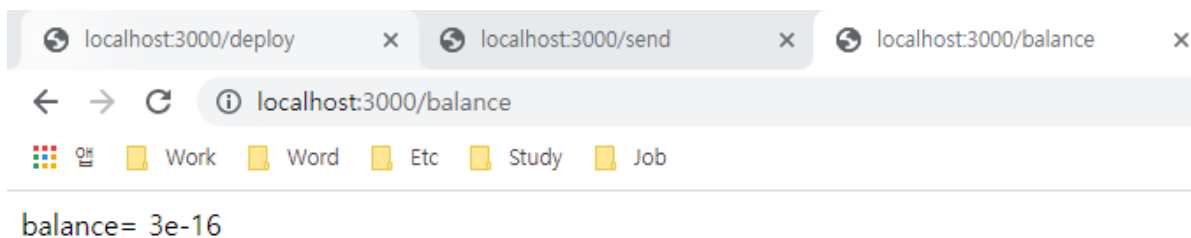
Send 결과



Balance 적용 완료 Decimal 적용 안된 상태



Decimal 적용



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

