MultiSIG 실습

태그	Multisig	Wallet

- 태그: 작성하려는 글에 맞거나 연관되어 있는 태그를 선택합니다.
- 상태: 해당 글의 상태를 의미합니다.
    - 글을 쓸 예정으로 등록했다면 `작성 예정`, 글을 쓰는 중이거나 아직 완료한 것 같지 않다면 `작성 중`, 완료 후에는 `완료`로 표기합니다.

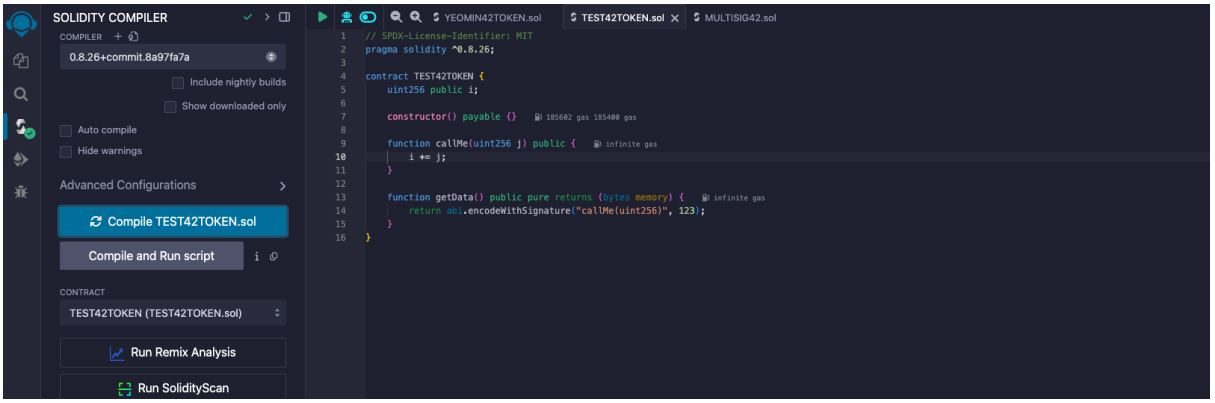
⚠가독성을 위해 개요와 결론을 작성하시는 것을 추천하지만, 느낌에 따라 자유롭게 작성하시면 됩니다!

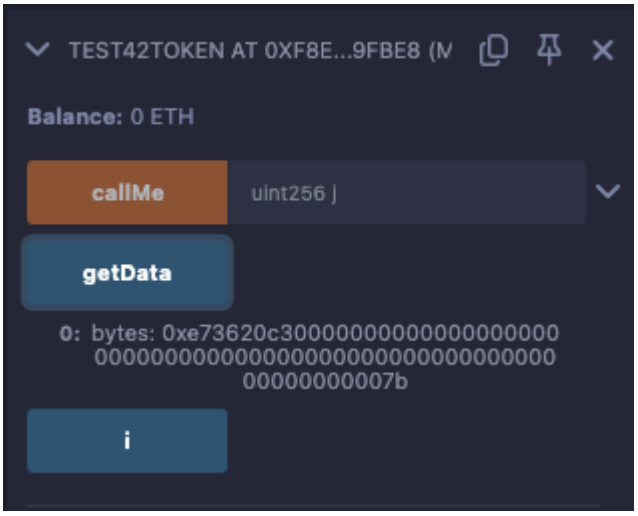
개요

본론

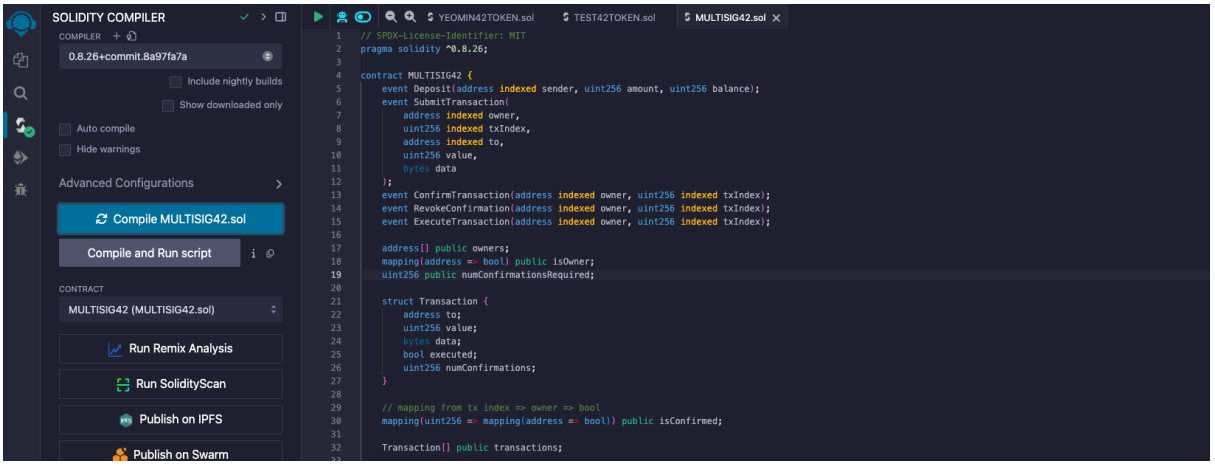
토큰 컴파일 및 배포

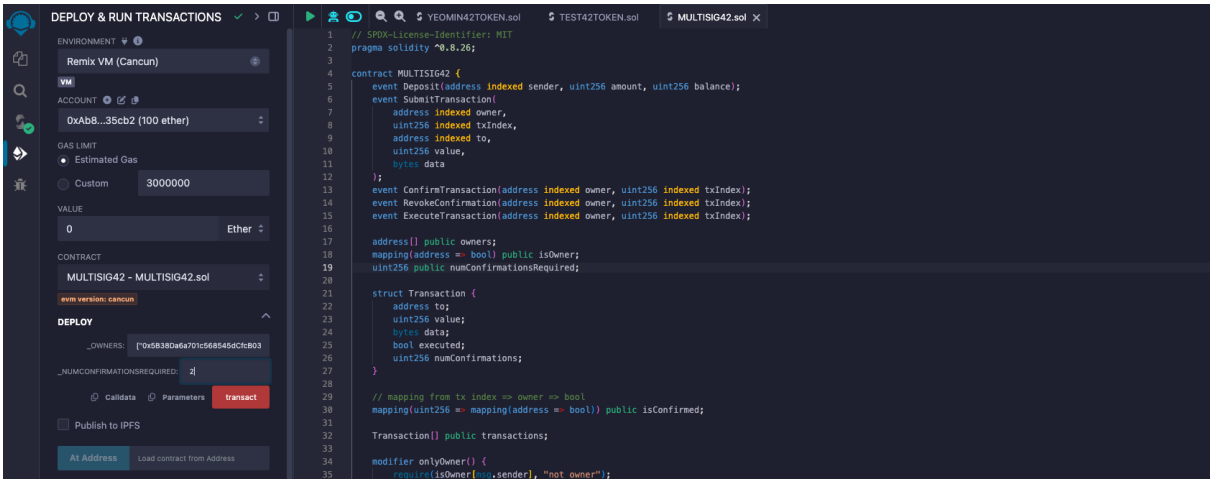
임시토큰



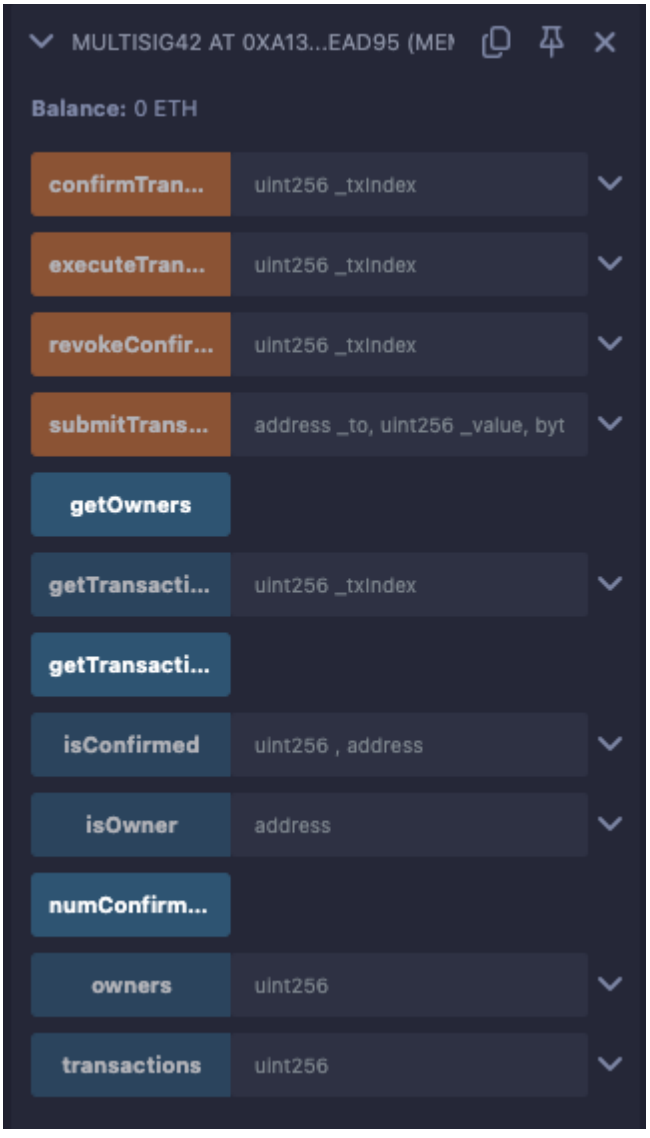


다중서명지갑 컴파일 및 배포



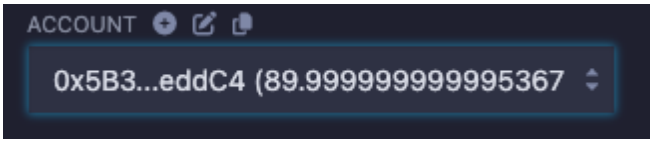


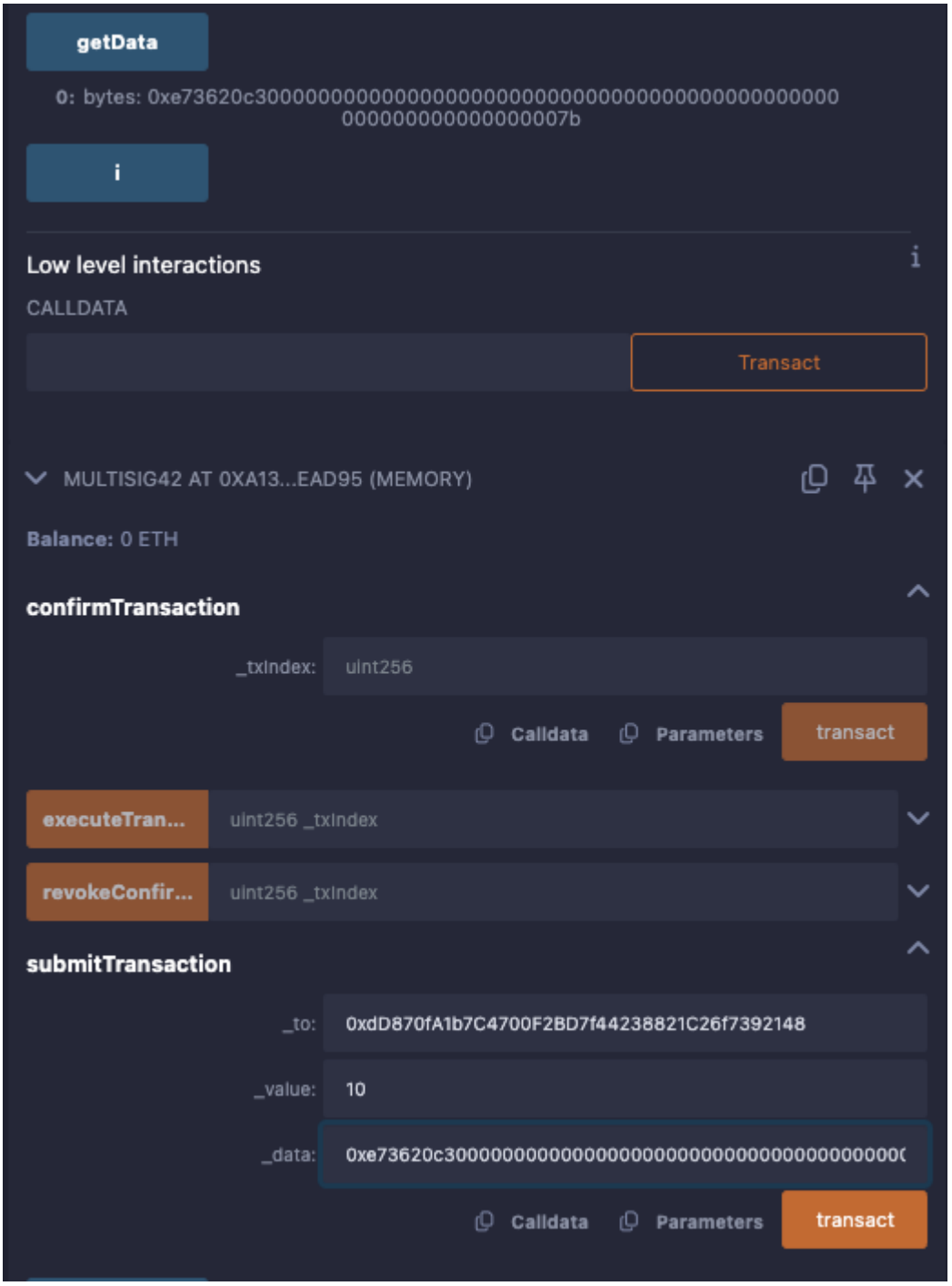

[vm] from: 0xAb8...35cb2 to: MULTISIG42.(constructor) value: 0 wei data: 0x608...35cb2 logs: 0 hash: 0x7dc...05f37
status 0x1 Transaction mined and execution succeed
transaction hash 0x7dc6a4a16dea50459d59bd037cf1a2675a71dedf6be7ffb990f466ad83c05f37
block hash 0xd6b91b9fcbd5d7fe9a9d0cc062eb230b3f7430a4ddac318d63f8dc626592af4a
block number 4
contract address 0xa131AD247055FD2e2aA8b156A11bdEc81b9eAD95
from 0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2
to MULTISIG42.(constructor)
gas 2110038 gas
transaction cost 1834815 gas
execution cost 1642017 gas
input 0x608...35cb2
decoded input
{
"address[] _owners": [
"0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
"0xAb8483F64d9C6d1EcF9b849Ae677dD3315835cb2"
],
"uint256 _numConfirmationsRequired": "2"
}
decoded output -
logs []


MULTISIG42 AT 0XA13...EAD95 (MEI
Balance: 0 ETH
confirmTran...
uint256 _txIndex
executeTran...
uint256 _txIndex
revokeConfir...
uint256 _txIndex
submitTrans...
address _to, uint256 _value, byt
getOwners
getTransacti...
uint256 _txIndex
getTransacti...
isConfirmed
uint256 , address
isOwner
address
numConfirm...
owners
uint256
transactions
uint256

전송 트랜잭션 생성

첫번째 소유자 트랜잭션 생성





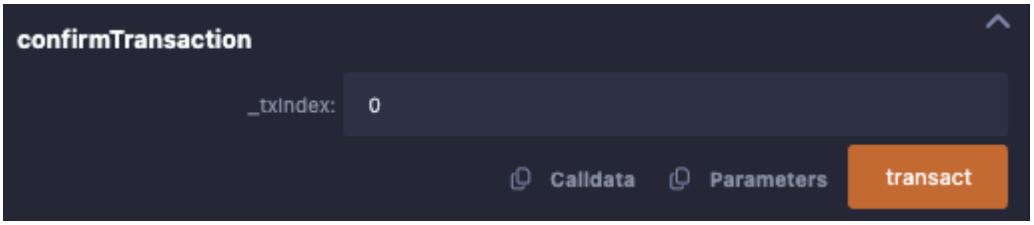
에러상황(Owner가 아닌 경우)

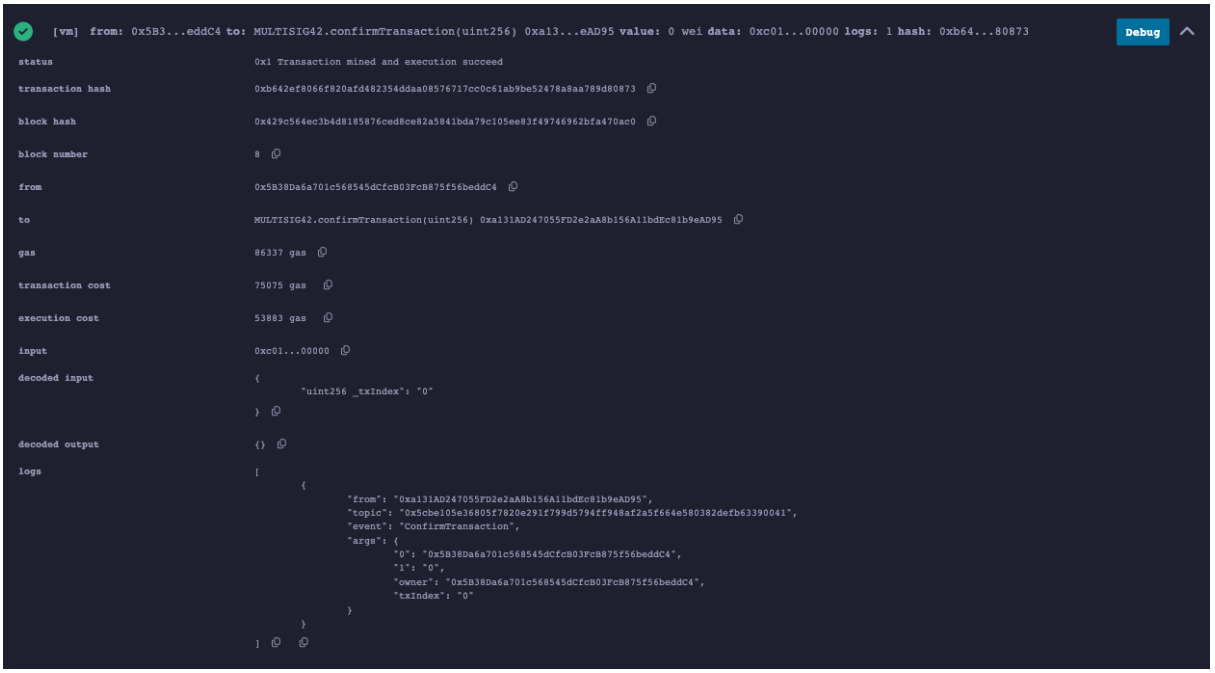
성공상황

트랜잭션 컨펌

첫번째 소유자 컨펌

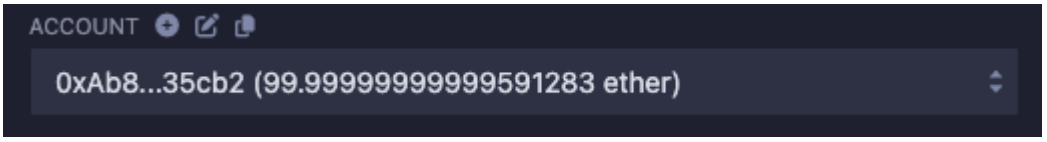
`isConfirmed` 를 이용해서 현재상황은 Confirmed되지 않았다는것을 확인할 수 있다.



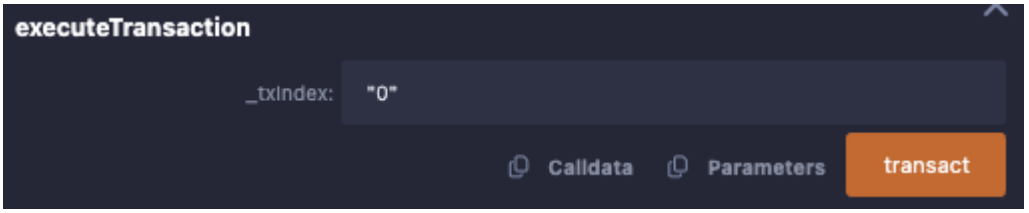


다시 `isConfirmed` 를 이용해서 확인하면 True로 바뀌어있음을 확인할 수 있다.

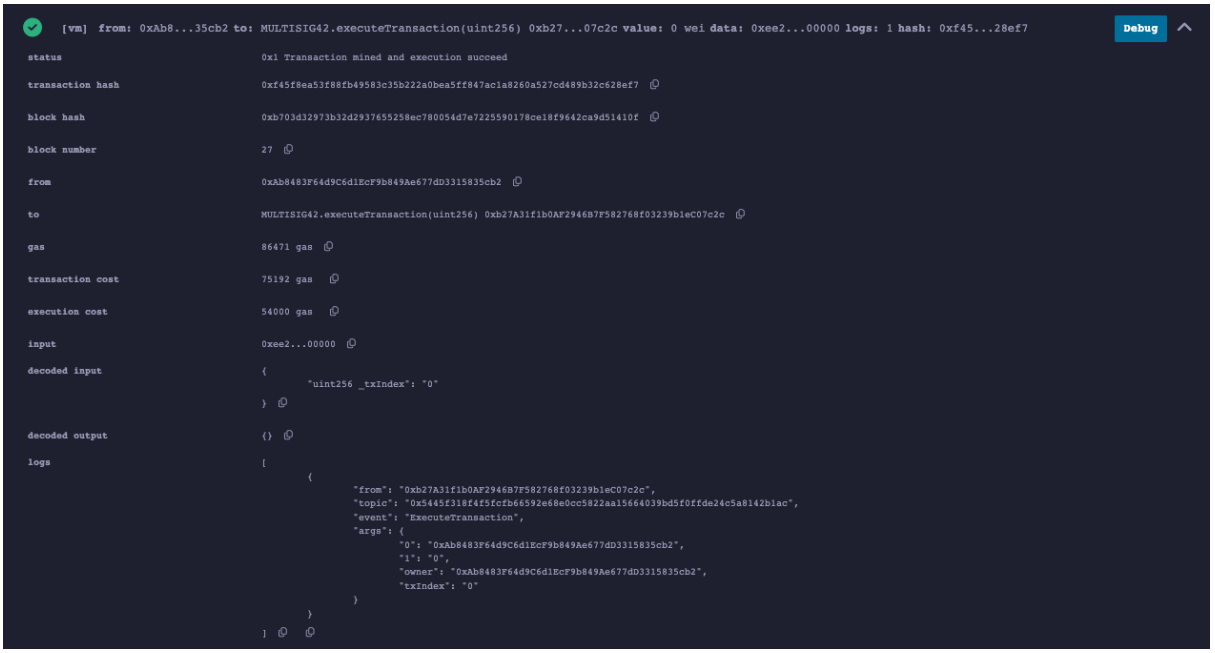
두번째 소유자 컨펌



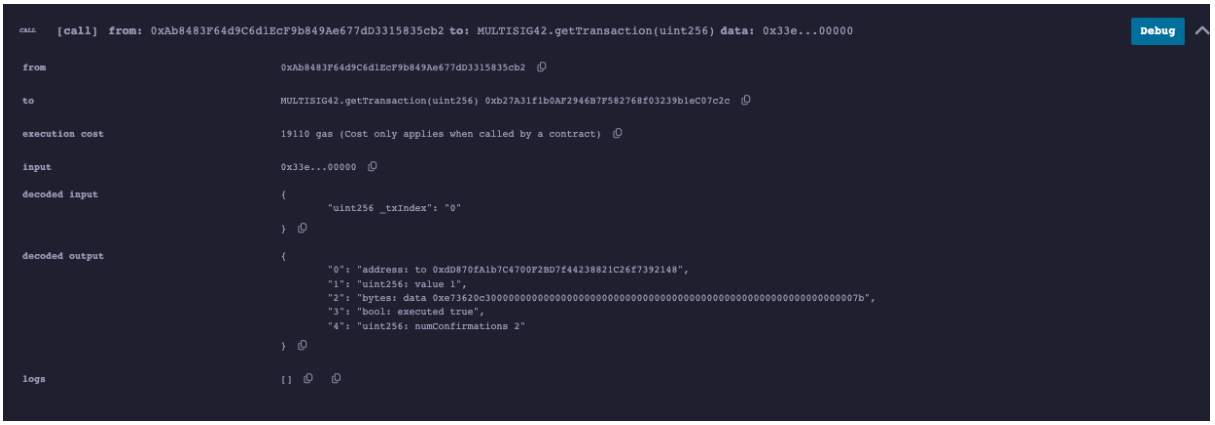
트랜잭션 실행



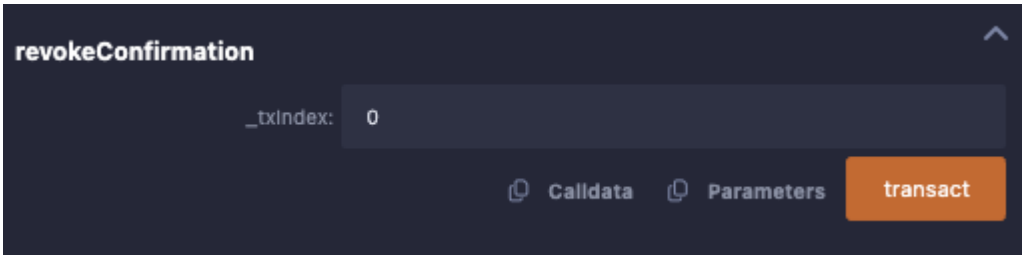
사용자 둘 중 한 명이라도 execute하면 됩니다.

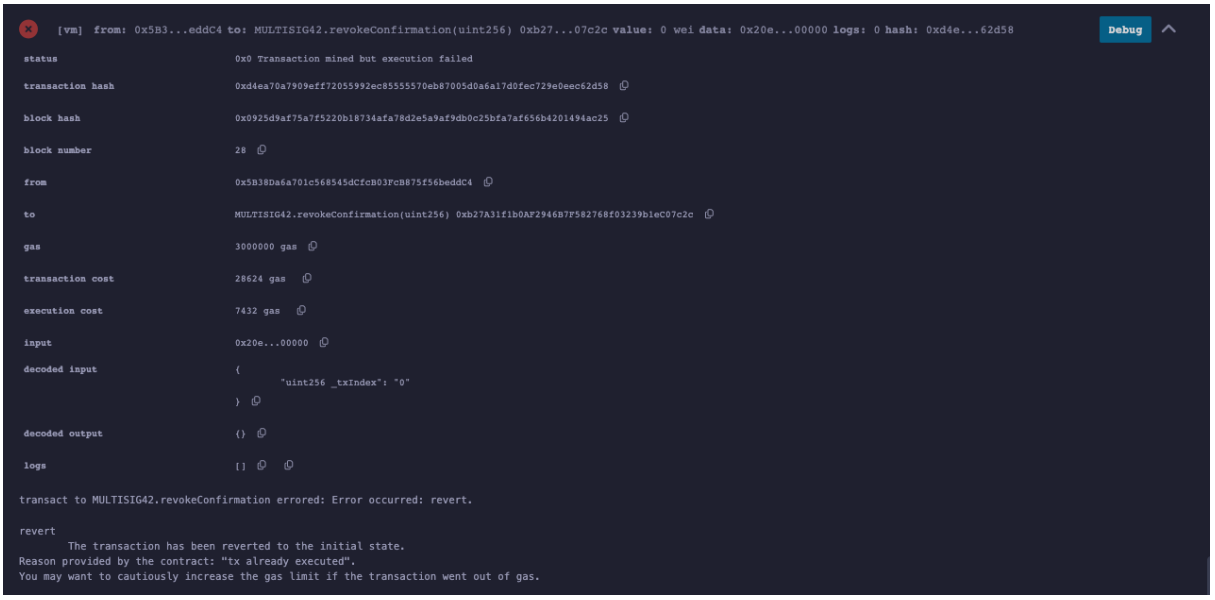


이제 `getTransaction`으로 정상적으로 execute되는지 확인해봅시다.



컨펌을 취소하려고 해도, 실행했다고 에러가 발생합니다.





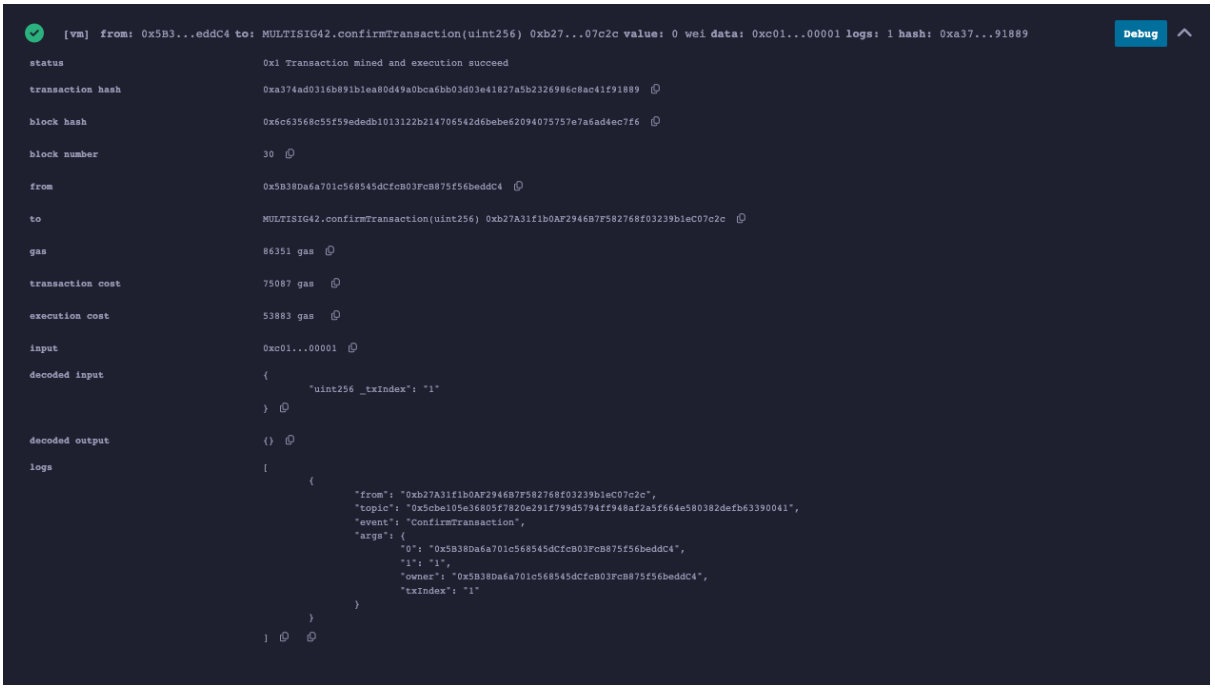
트랜잭션 컨펌 취소

새로운 트랜잭션을 만들고 컨펌을 한 후 취소해보겠습니다.

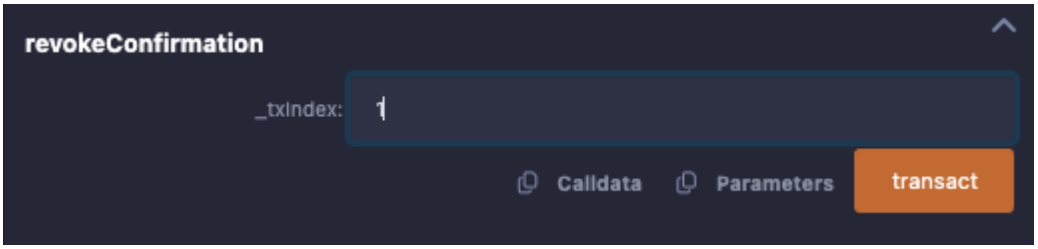
트랜잭션 신청


[vm] from: 0x5B3...eddC4 to: MULTISIG42.submitTransaction(address,uint256,bytes) 0xb27...07c2c value: 0 wei data: 0xc64...00000 logs: 1 hash: 0x9a5...2cbbe
Debug
status
0x1 Transaction mined and execution succeed
transaction hash
0x9a55adb6655864b6f39f6b88e94a4f7580425beecfde88e675c1d1c2d772cbbe
block hash
0x2044a34c85de2d7a71fc431623164f25fff3b6bb760ccbf45a5e83783e7dcf20
block number
29
from
0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to
MULTISIG42.submitTransaction(address,uint256,bytes) 0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c
gas
173415 gas
transaction cost
150795 gas
execution cost
128627 gas
input
0xc64...00000
decoded input
{
"address _to": "0xdD870fA1b7C4700F2BD7f44238821C26f7392148",
"uint256 _value": "1",
"bytes _data": "0xe73620c3000000000000000000000000000000000000000000000000000000000000007b"
}
decoded output
{}
logs
[
{
"from": "0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c",
"topic": "0xd5a05bf70715ad82a09a756320284a1b54c9ff74cd0f8cce6219e79b563fe59d",
"event": "SubmitTransaction",
"args": {
"0": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
"1": "1",
"2": "0xdD870fA1b7C4700F2BD7f44238821C26f7392148",
"3": "1",
"4": "0xe73620c3000000000000000000000000000000000000000000000000000000000000007b",
"owner": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
"txIndex": "1",
"to": "0xdD870fA1b7C4700F2BD7f44238821C26f7392148",
"value": "1",
"data": "0xe73620c3000000000000000000000000000000000000000000000000000000000000007b"
}
}
]

트랜잭션 컨펌


[vm] from: 0x5B3...eddC4 to: MULTISIG42.confirmTransaction(uint256) 0xb27...07c2c value: 0 wei data: 0xc01...00001 logs: 1 hash: 0xa37...91889
Debug
status
0x1 Transaction mined and execution succeed
transaction hash
0xa374ad0316b891b1ea80d49a0bca6bb03d03e41827a5b2326986c8ac41f91889
block hash
0x6c63568c55f59ededb1013122b214706542d6bebe62094075757e7a6ad4ec7f6
block number
30
from
0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to
MULTISIG42.confirmTransaction(uint256) 0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c
gas
86351 gas
transaction cost
75087 gas
execution cost
53883 gas
input
0xc01...00001
decoded input
{
"uint256 _txIndex": "1"
}
decoded output
{}
logs
[
{
"from": "0xb27A31f1b0AF2946B7F582768f03239b1eC07c2c",
"topic": "0x5cbe105e36805f7820e291f799d5794ff948af2a5f664e580382defb63390041",
"event": "ConfirmTransaction",
"args": {
"0": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
"1": "1",
"owner": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4",
"txIndex": "1"
}
}
]

컨펌 취소



다시 시도했을때 컨펌이 안되어있다는 에러가 발생합니다.

결론

멀티시그가 지원되는 지갑형태의 컨트랙트를 만든 후 테스트 토큰을 통해서 다중시그가 어떻게 구현되는지 확인해봤습니다.

참고

참고했습니다..