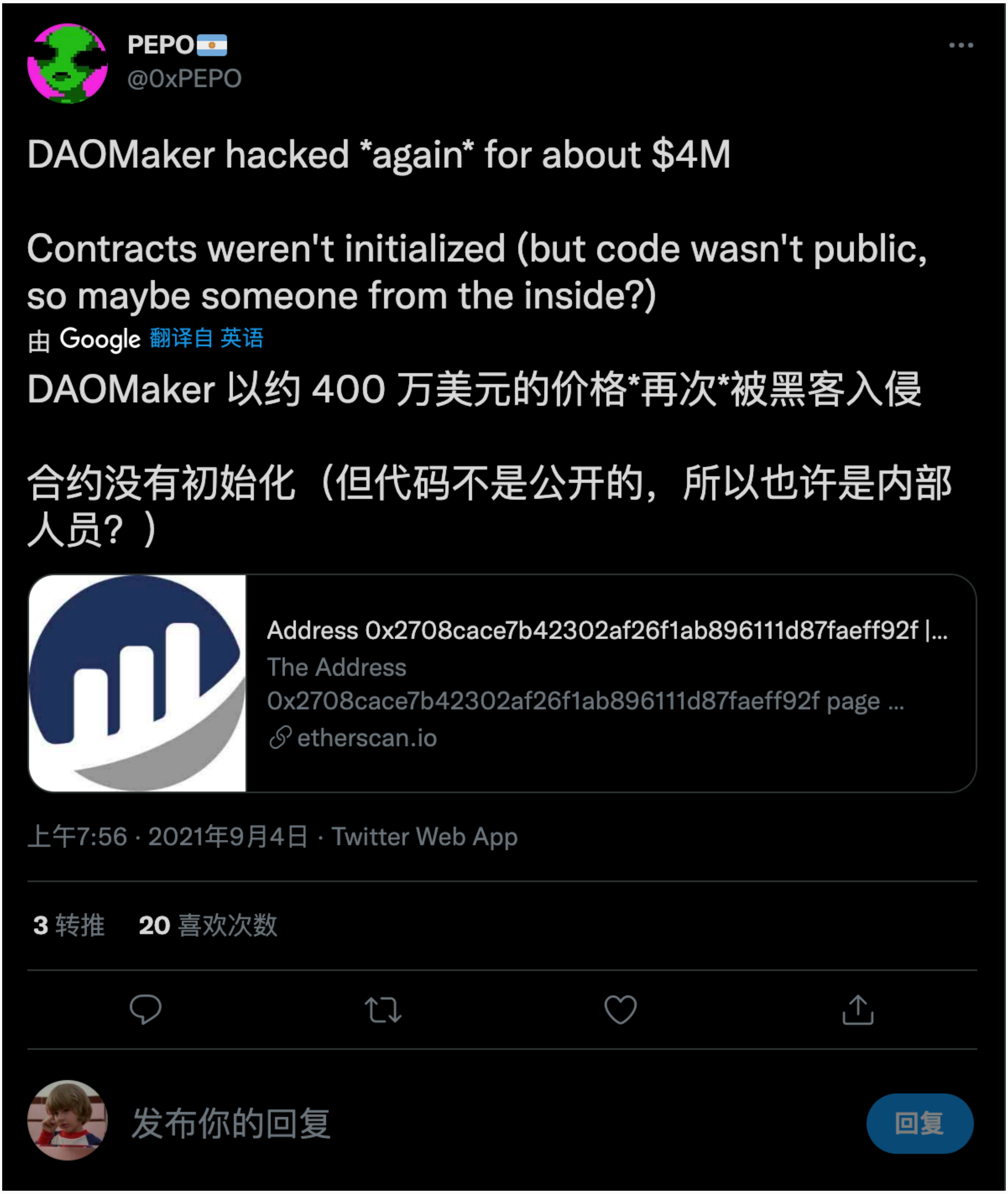
DAO MAKER HACKED

前言

> - Author: xxxeyJ@BlockCrisis
> - Blog: tricksongs.com



PEPO
@0xPEPO

DAOMaker hacked *again* for about $4M

Contracts weren't initialized (but code wasn't public, so maybe someone from the inside?)

由 Google 翻译自 英语

DAOMaker 以约 400 万美元的价格*再次*被黑客入侵

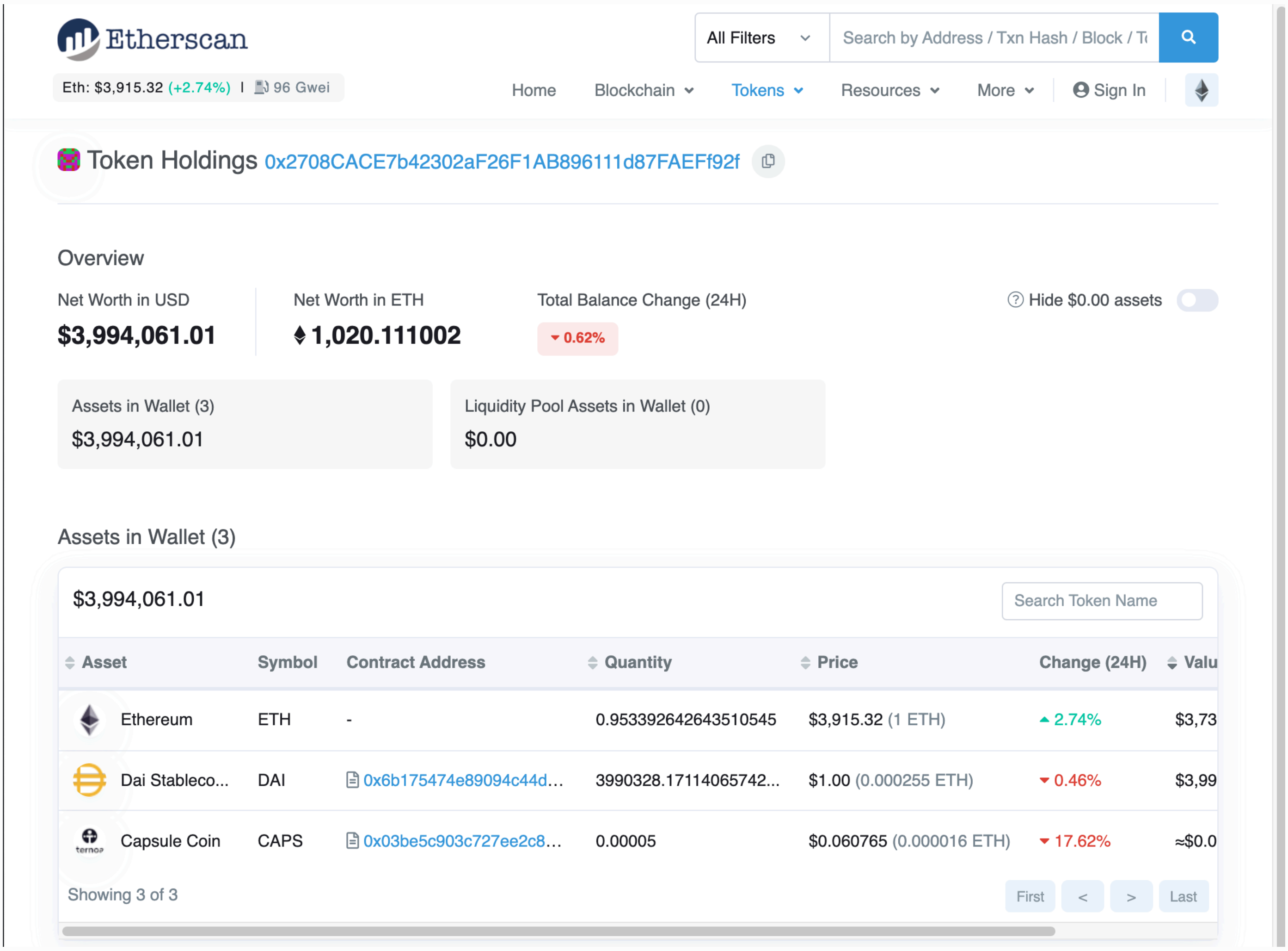
合约没有初始化（但代码不是公开的，所以也许是内部人员？）

Address 0x2708cace7b42302af26f1ab896111d87faeff92f |...
The Address 0x2708cace7b42302af26f1ab896111d87faeff92f page ...
etherscan.io

上午7:56 · 2021年9月4日 · Twitter Web App

3 转推 20 喜欢次数

据推特安全事件披露，DAO Maker 遭受黑客攻击，攻击者利用智能合约中的初始化方法中鉴权部分所存在的漏洞将自身角色提升为特权账户后进而通过调用 `emergencyExit()` ，窃取了一系列 Token 并最终兑换为将近 $400w DAI 稳定币获利走人


Etherscan
All Filters
Search by Address / Txn Hash / Block / To
Eth: $3,915.32 (+2.74%) | 96 Gwei
Home
Blockchain
Tokens
Resources
More
Sign In

Token Holdings 0x2708CACE7b42302aF26F1AB896111d87FAEFf92f

Overview

Net Worth in USD
$3,994,061.01

Net Worth in ETH
1,020.111002

Total Balance Change (24H)
0.62%

Hide $0.00 assets

Assets in Wallet (3)
$3,994,061.01

Liquidity Pool Assets in Wallet (0)
$0.00

Assets in Wallet (3)

$3,994,061.01

Asset	Symbol	Contract Address	Quantity	Price	Change (24H)	Valu
Ethereum	ETH	-	0.953392642643510545	$3,915.32 (1 ETH)	▲ 2.74%	$3,73
Dai Stableco...	DAI	0x6b175474e89094c44d...	3990328.17114065742...	$1.00 (0.000255 ETH)	▼ 0.46%	$3,99
Capsule Coin	CAPS	0x03be5c903c727ee2c8...	0.00005	$0.060765 (0.000016 ETH)	▼ 17.62%	≈$0.0

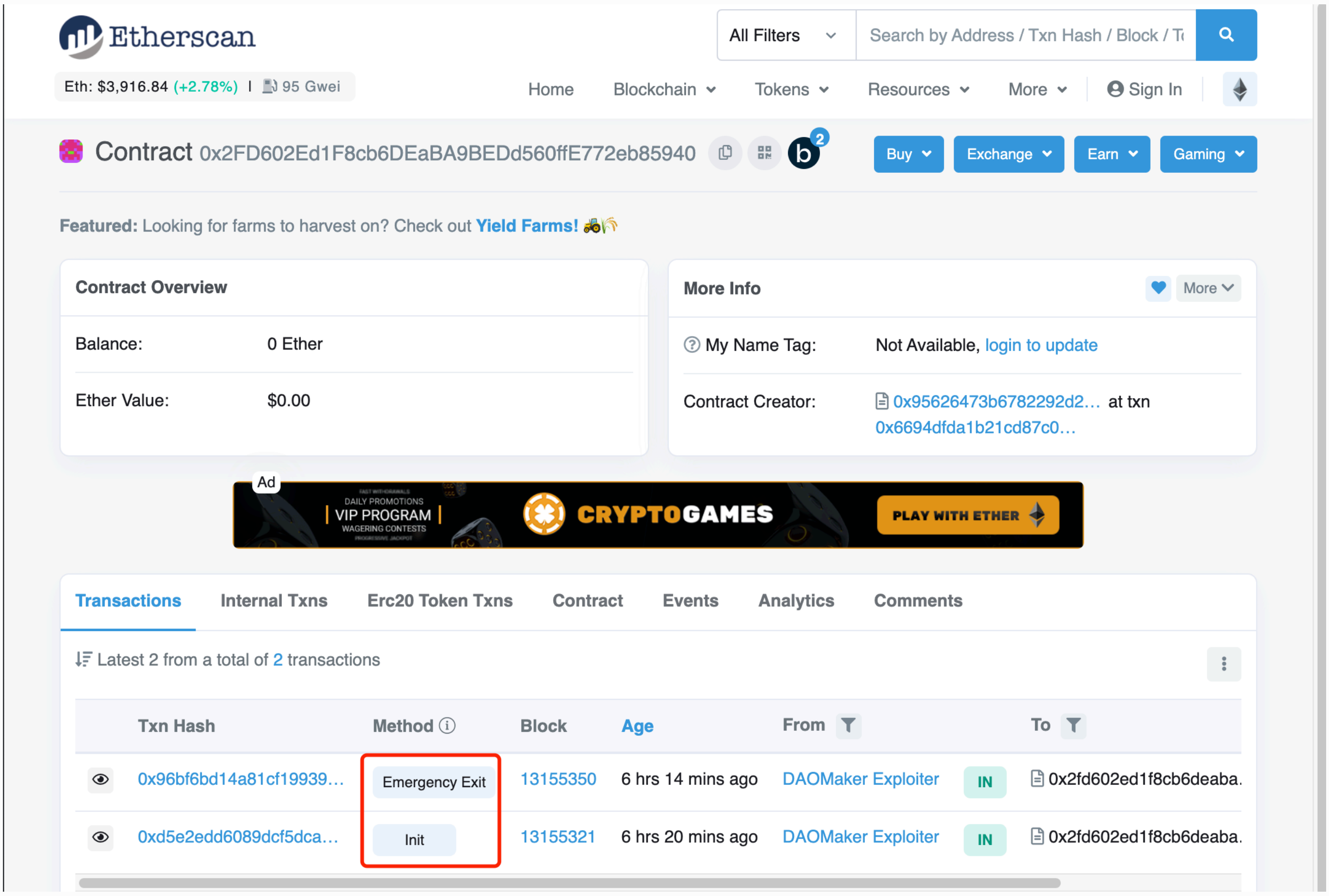
Showing 3 of 3

涉事账户

黑客地址(EOA): 0x2708cace7b42302af26f1ab896111d87faeff92f
代理合约: 0x2fd602ed1f8cb6deaba9bedd560ffe772eb85940 &
0xdd571023d95ff6ce5716bf112ccb752e86212167
逻辑合约: 0xf17ca0e0f24a5fa27944275fa0cedec24fbf8ee2

ATTACK TRACE

攻击者调用初始化方法的Tx Hash:
0xd5e2edd6089dcf5dca78c0ccbdf659acedab173a8ab3cb65720e35b640c0af7c



Contract 0x2FD602Ed1F8cb6DEaBA9BEDd560ffE772eb85940

Featured: Looking for farms to harvest on? Check out **Yield Farms!**

Contract Overview

Balance: 0 Ether

Ether Value: $0.00

More Info

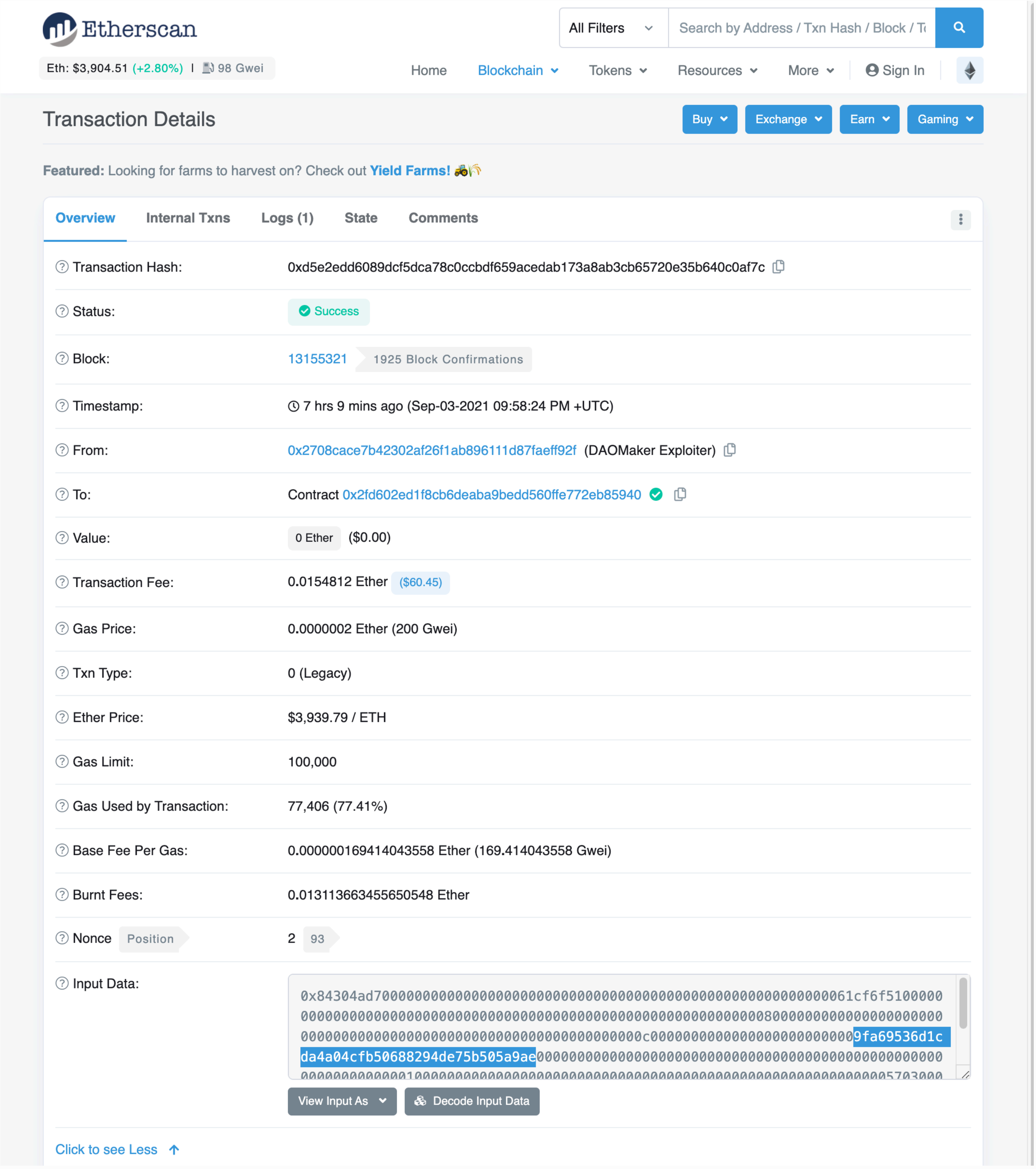
My Name Tag: Not Available, login to update

Contract Creator: 0x95626473b6782292d2… at txn 0x6694dfda1b21cd87c0…

Latest 2 from a total of 2 transactions

Txn Hash	Method	Block	Age	From		To
0x96bf6bd14a81cf19939…	Emergency Exit	13155350	6 hrs 14 mins ago	DAOMaker Exploiter	IN	0x2fd602ed1f8cb6deaba.
0xd5e2edd6089dcf5dca…	Init	13155321	6 hrs 20 mins ago	DAOMaker Exploiter	IN	0x2fd602ed1f8cb6deaba.

由于智能合约未对 `init()` 进行防护，所以攻击者通过 Calldata 指定调用 **init()** function 进而成为了逻辑合约的特权账户， init() 函数签名为 `0x84304ad7` ，传递指定 Token：0x9fa69536d1cda4a04cfb50688294de75b505a9ae(DERC)



Transaction Details

Featured: Looking for farms to harvest on? Check out Yield Farms!

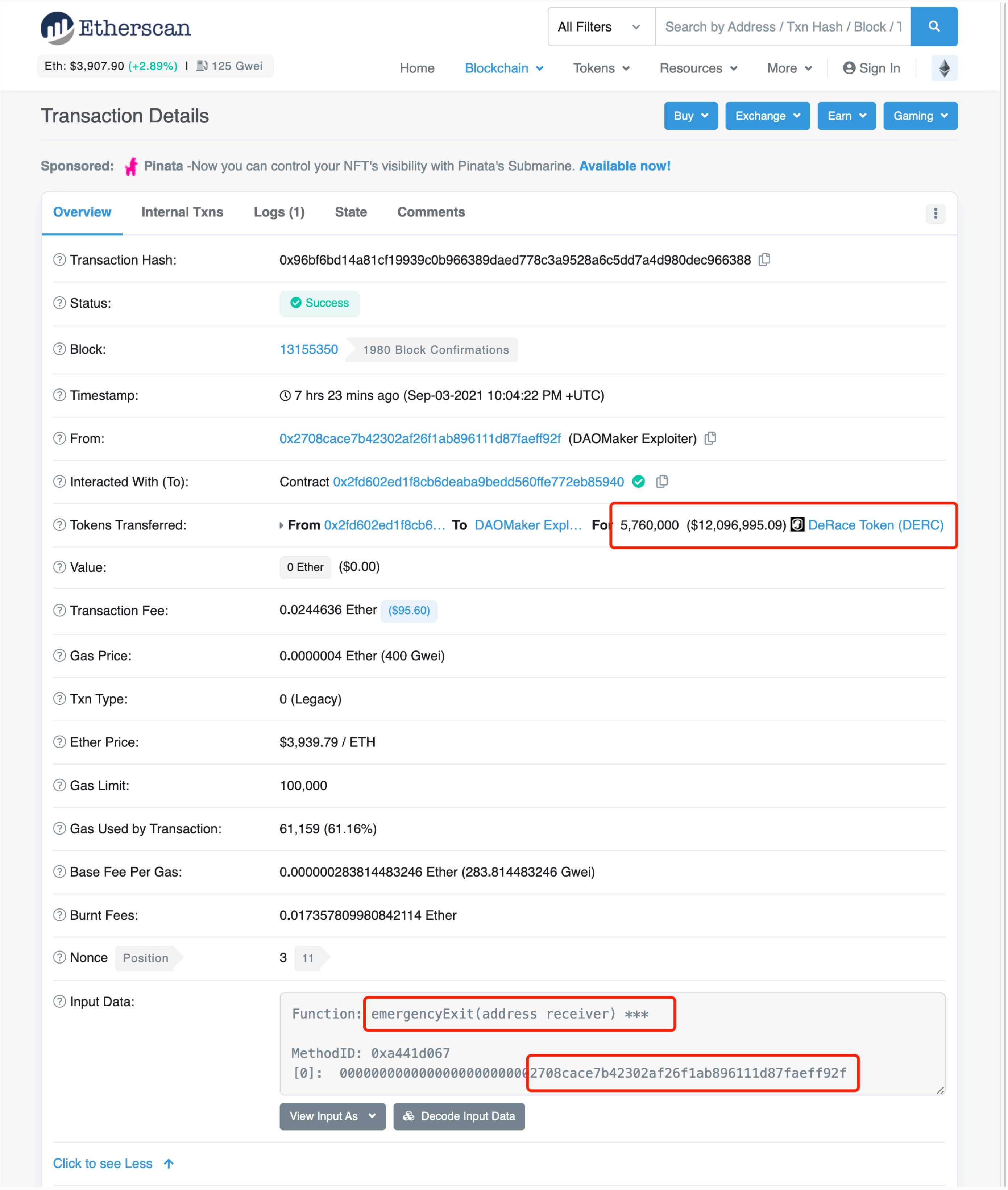
Transaction Hash:	0xd5e2edd6089dcf5dca78c0ccbdf659acedab173a8ab3cb65720e35b640c0af7c
Status:	Success
Block:	13155321 1925 Block Confirmations
Timestamp:	7 hrs 9 mins ago (Sep-03-2021 09:58:24 PM +UTC)
From:	0x2708cace7b42302af26f1ab896111d87faeff92f (DAOMaker Exploiter)
To:	Contract 0x2fd602ed1f8cb6deaba9bedd560ffe772eb85940
Value:	0 Ether ($0.00)
Transaction Fee:	0.0154812 Ether ($60.45)
Gas Price:	0.0000002 Ether (200 Gwei)
Txn Type:	0 (Legacy)
Ether Price:	$3,939.79 / ETH
Gas Limit:	100,000
Gas Used by Transaction:	77,406 (77.41%)
Base Fee Per Gas:	0.000000169414043558 Ether (169.414043558 Gwei)
Burnt Fees:	0.013113663455650548 Ether
Nonce Position	2 93
Input Data:	

```
0x84304ad7000000000000000000000000000000000000000000000000000000000061cf6f5100000
0000000000000000000000000000000000000000000000000000000008000000000000000000000
000000000000000000000000000000000000000000c00000000000000000000000009fa69536d1c
da4a04cfb50688294de75b505a9ae00000000000000000000000000000000000000000000000000
0000000000000100000000000000000000000000000000000000000000000000000000005703000
```

而后攻击者通过调用 **emergencyExit()** function 传递 `receiver` 参数为攻击者地址进行提款，**emergencyExit()** 的函数签名为：0xa441d067

该笔交易的 Tx Hash 为:

0x96bf6bd14a81cf19939c0b966389daed778c3a9528a6c5dd7a4d980dec966388



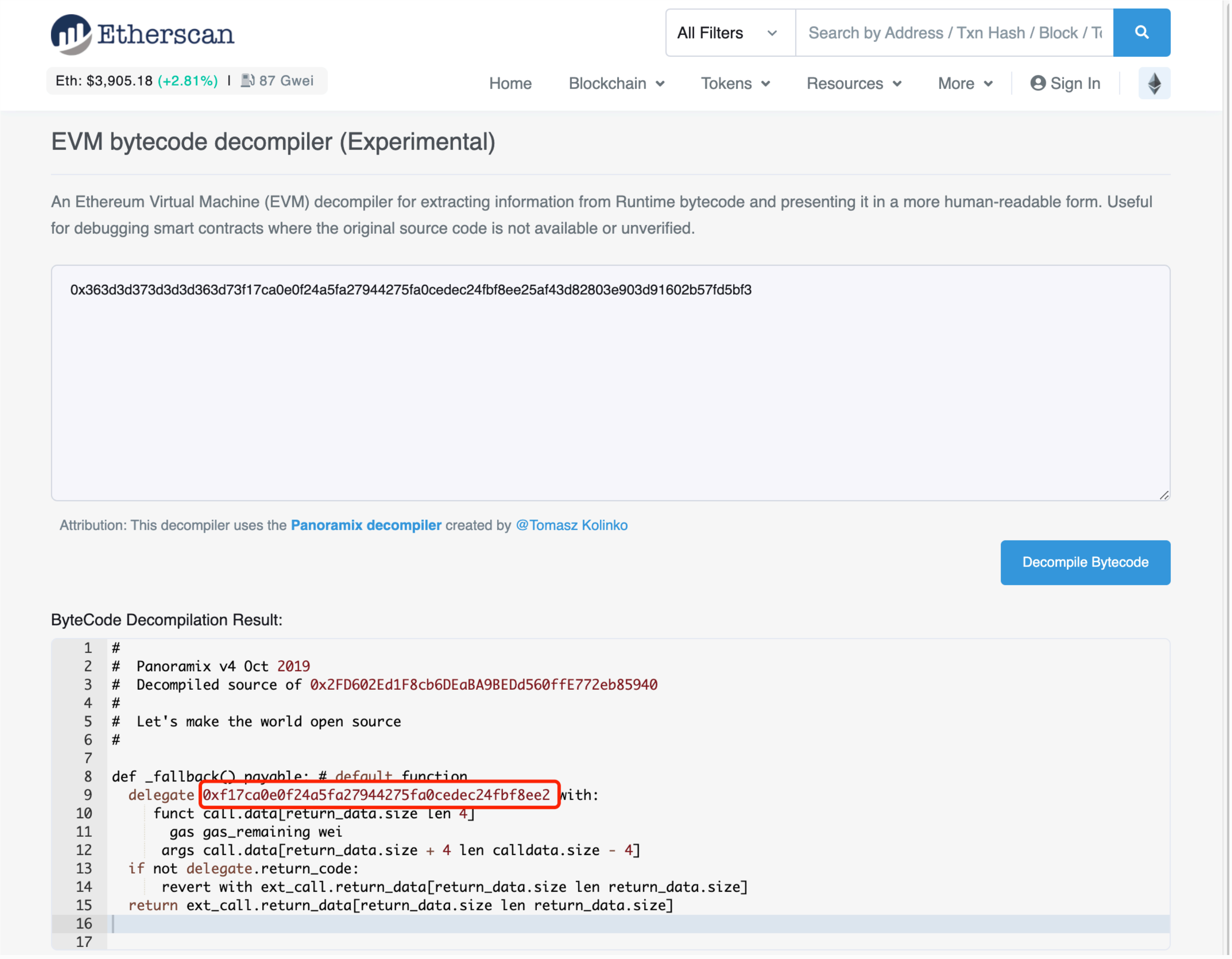
Transaction Details

Sponsored: Pinata -Now you can control your NFT's visibility with Pinata's Submarine. **Available now!**

Transaction Hash:	0x96bf6bd14a81cf19939c0b966389daed778c3a9528a6c5dd7a4d980dec966388
Status:	Success
Block:	13155350 1980 Block Confirmations
Timestamp:	7 hrs 23 mins ago (Sep-03-2021 10:04:22 PM +UTC)
From:	0x2708cace7b42302af26f1ab896111d87faeff92f (DAOMaker Exploiter)
Interacted With (To):	Contract 0x2fd602ed1f8cb6deaba9bedd560ffe772eb85940
Tokens Transferred:	**From** 0x2fd602ed1f8cb6... **To** DAOMaker Expl... **For** 5,760,000 ($12,096,995.09) DeRace Token (DERC)
Value:	0 Ether ($0.00)
Transaction Fee:	0.0244636 Ether ($95.60)
Gas Price:	0.0000004 Ether (400 Gwei)
Txn Type:	0 (Legacy)
Ether Price:	$3,939.79 / ETH
Gas Limit:	100,000
Gas Used by Transaction:	61,159 (61.16%)
Base Fee Per Gas:	0.000000283814483246 Ether (283.814483246 Gwei)
Burnt Fees:	0.017357809980842114 Ether
Nonce Position	3 11
Input Data:	Function: emergencyExit(address receiver) *** MethodID: 0xa441d067 [0]: 0000000000000000000000002708cace7b42302af26f1ab896111d87faeff92f

由于代理合约未开源，所以对代理合约进行反编译发现对应的逻辑合约为：

0xf17ca0e0f24a5fa27944275fa0cedec24fbf8ee2



Etherscan
Eth: $3,905.18 (+2.81%) | 87 Gwei
All Filters
Search by Address / Txn Hash / Block / To
Home
Blockchain
Tokens
Resources
More
Sign In

EVM bytecode decompiler (Experimental)

An Ethereum Virtual Machine (EVM) decompiler for extracting information from Runtime bytecode and presenting it in a more human-readable form. Useful for debugging smart contracts where the original source code is not available or unverified.

0x363d3d373d3d3d363d73f17ca0e0f24a5fa27944275fa0cedec24fbf8ee25af43d82803e903d91602b57fd5bf3

Attribution: This decompiler uses the **Panoramix decompiler** created by @Tomasz Kolinko

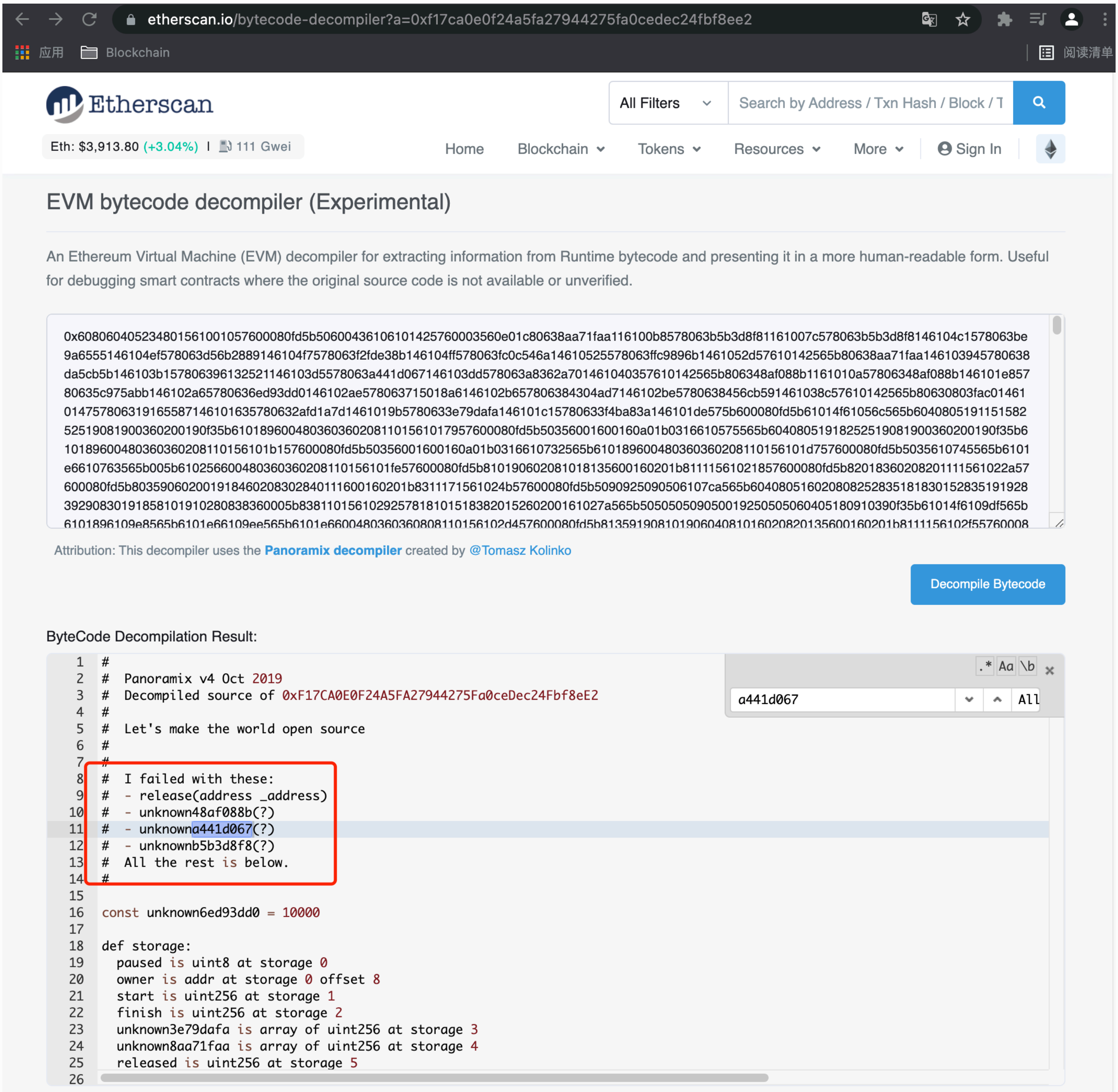
ByteCode Decompilation Result:

```
#
#  Panoramix v4 Oct 2019
#  Decompiled source of 0x2FD602Ed1F8cb6DEaBA9BEDd560ffE772eb85940
#
#  Let's make the world open source
#

def _fallback() payable: # default function
  delegate 0xf17ca0e0f24a5fa27944275fa0cedec24fbf8ee2 with:
     funct call.data[return_data.size len 4]
       gas gas_remaining wei
      args call.data[return_data.size + 4 len calldata.size - 4]
  if not delegate.return_code:
      revert with ext_call.return_data[return_data.size len return_data.size]
  return ext_call.return_data[return_data.size len return_data.size]

```

并且逻辑合约也处于未开源状态，因此猜测此次攻击事件很有可能是项目方作恶



etherscan.io/bytecode-decompiler?a=0xf17ca0e0f24a5fa27944275fa0cedec24fbf8ee2
应用
Blockchain
阅读清单
Etherscan
All Filters
Search by Address / Txn Hash / Block / T
Eth: $3,913.80 (+3.04%) | 111 Gwei
Home
Blockchain
Tokens
Resources
More
Sign In

EVM bytecode decompiler (Experimental)

An Ethereum Virtual Machine (EVM) decompiler for extracting information from Runtime bytecode and presenting it in a more human-readable form. Useful for debugging smart contracts where the original source code is not available or unverified.

```
0x608060405234801561001057600080fd5b50600436106101425760003560e01c80638aa71faa116100b8578063b5b3d8f81161007c578063b5b3d8f8146104c1578063be
9a6555146104ef578063d56b2889146104f7578063f2fde38b146104ff578063fc0c546a14610525578063ffc9896b1461052d57610142565b80638aa71faa146103945780638
da5cb5b146103b157806396132521146103d5578063a441d067146103dd578063a8362a701461040357610142565b806348af088b1161010a57806348af088b146101e857
80635c975abb146102a65780636ed93dd0146102ae578063715018a6146102b657806384304ad7146102be5780638456cb591461038c57610142565b80630803fac01461
0147578063191655871461016357806332afd1a7d1461019b5780633e79dafa146101c15780633f4ba83a146101de575b600080fd5b61014f61056c565b6040805191151582
52519081900360200190f35b61018960048036036020811015610179576000 80fd5b50356001600160a01b0316610575565b60408051918252519081900360200190f35b6
10189600480360360208110156101b157600080fd5b50356001600160a01b0316610732565b610189600480360360208110156101d757600080fd5b5035610745565b6101
e6610763565b005b61025660048036036020811015610 1fe57600080fd5b810190602081018135600160201b81111561021857600080fd5b82018360208201111561022a57
600080fd5b803590602001918460208302840111600160201b8311171561024b57600080fd5b5090925090506107ca565b604080516020808252835181830152835191928
392908301918581019102808383600 05b838110156102925781810151838201526020016102 7a565b505050509050019250505060405180910390f35b61014f6109df565b
6101896109e8565b6101e66109ee565b6101e6600480360360808110156102d457600080fd5b81359190810190604081016020820135600160201b8111156102f55760008
```

Attribution: This decompiler uses the **Panoramix decompiler** created by @Tomasz Kolinko

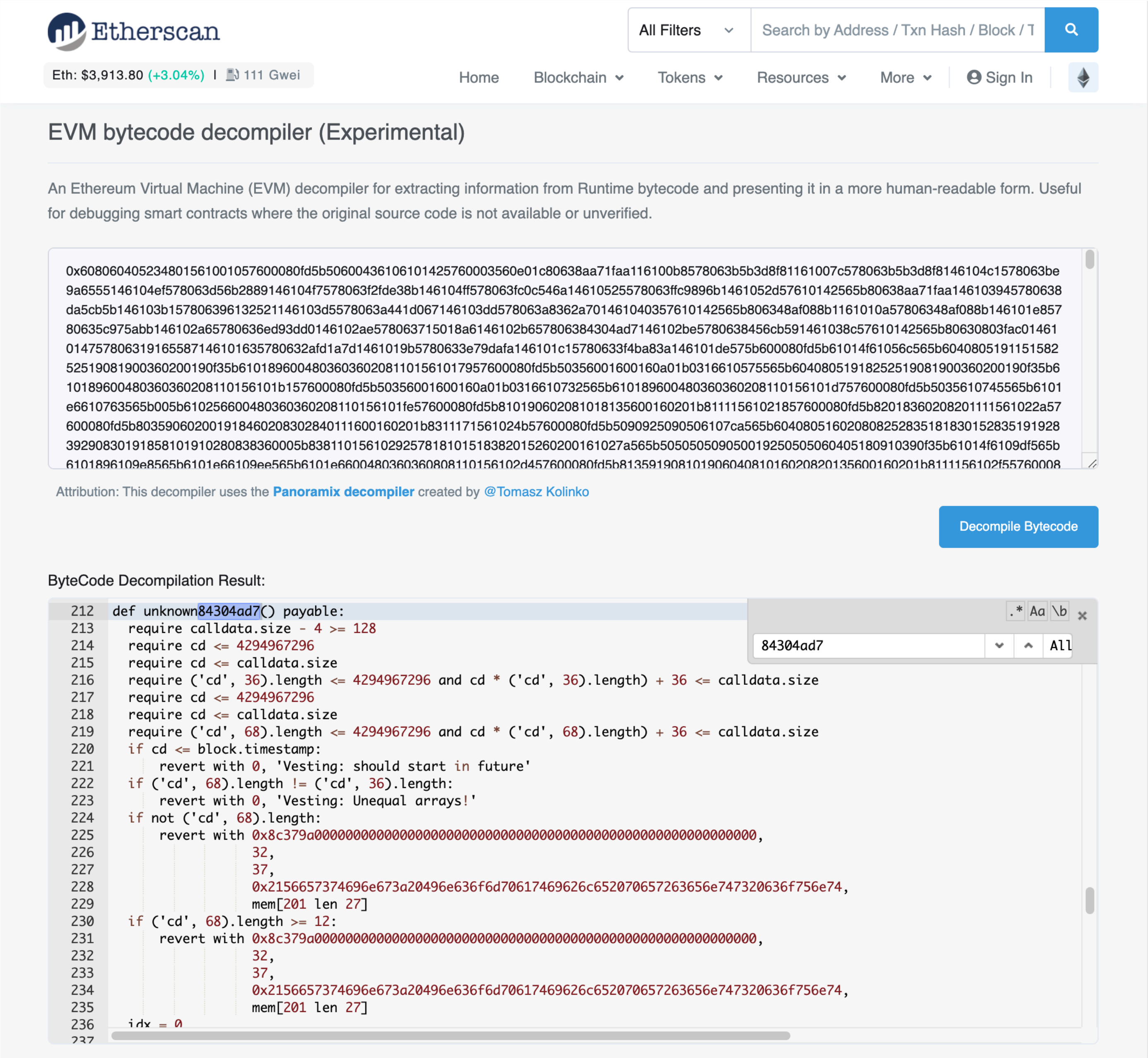
ByteCode Decompilation Result:

```
#
#  Panoramix v4 Oct 2019
#  Decompiled source of 0xF17CA0E0F24A5FA27944275Fa0ceDec24Fbf8eE2
#
#  Let's make the world open source
#
#
#  I failed with these:
#  - release(address _address)
#  - unknown48af088b(?)
#  - unknowna441d067(?)
#  - unknownb5b3d8f8(?)
#  All the rest is below.
#

const unknown6ed93dd0 = 10000

def storage:
  paused is uint8 at storage 0
  owner is addr at storage 0 offset 8
  start is uint256 at storage 1
  finish is uint256 at storage 2
  unknown3e79dafa is array of uint256 at storage 3
  unknown8aa71faa is array of uint256 at storage 4
  released is uint256 at storage 5

```



EVM bytecode decompiler (Experimental)

An Ethereum Virtual Machine (EVM) decompiler for extracting information from Runtime bytecode and presenting it in a more human-readable form. Useful for debugging smart contracts where the original source code is not available or unverified.

```
0x608060405234801561001057600080fd5b50600436106101425760003560e01c80638aa71faa116100b8578063b5b3d8f81161007c578063b5b3d8f8146104c1578063be
9a6555146104ef578063d56b2889146104f7578063f2fde38b146104ff578063fc0c546a1461052557806ffc9896b1461052d57610142565b80638aa71faa146103945780638
da5cb5b146103b1578063961325211461 03d5578063a441d067146103dd578063a8362a70146104035761 0142565b806348af088b1161010a57806348af088b146101e857
80635c975abb146102a65780636ed93dd0146102ae578063715018a6146102b657806384304ad7146102be5780638456cb591461038c57610142565b80630803fac01461
0147578063191655871461016357806 32afd1a7d1461019b5780633e79dafa146101c15780633f4ba83a146101de575b600080fd5b61014f61056c565b6040805191151582
52519081900360200190f35b61018960048036036020811015610179576000 80fd5b503560016001 60a01b0316610575565b6040805191825251908190036020 0190f35b6
101896004803603602081101561 01b157600080fd5b503560016001 60a01b0316610732565b610189600480360360208110156101d757600080fd5b5035610745565b6101
e6610763565b005b610256600480360360208110156101fe57600080fd5b8101906020810181356401 00000000811115610218576000 80fd5b82018360208201111561022a57
600080fd5b80359060200191846020830284011164010000000083111715610 24b57600080fd5b509092509050610 7ca565b604080516020808252835181830152835191928
39290830191858101910280838360005b8381101561029257818101518382015260200161027a565b505050509050019250505060405180910390f35b61014f6109df565b
6101896109e8565b6101e66109ee565b6101e66004803603608081101561 02d457600080fd5b81359190810190604081016020820135640100000000811115610 2f55760008
```

Attribution: This decompiler uses the **Panoramix decompiler** created by @Tomasz Kolinko

ByteCode Decompilation Result:

```
def unknown84304ad7() payable:
  require calldata.size - 4 >= 128
  require cd <= 4294967296
  require cd <= calldata.size
  require ('cd', 36).length <= 4294967296 and cd * ('cd', 36).length) + 36 <= calldata.size
  require cd <= 4294967296
  require cd <= calldata.size
  require ('cd', 68).length <= 4294967296 and cd * ('cd', 68).length) + 36 <= calldata.size
  if cd <= block.timestamp:
      revert with 0, 'Vesting: should start in future'
  if ('cd', 68).length != ('cd', 36).length:
      revert with 0, 'Vesting: Unequal arrays!'
  if not ('cd', 68).length:
      revert with 0x8c379a000000000000000000000000000000000000000000000000000000000,
                  32,
                  37,
                  0x2156657374696e673a20496e636f6d70617469626c652070657263656e747320636f756e74,
                  mem[201 len 27]
  if ('cd', 68).length >= 12:
      revert with 0x8c379a000000000000000000000000000000000000000000000000000000000,
                  32,
                  37,
                  0x2156657374696e673a20496e636f6d70617469626c652070657263656e747320636f756e74,
                  mem[201 len 27]
  idx = 0
```