



Blockchain Autopsies: Analyzing selfdestructs

Jay Little
devcon4
November 1, 2018

Sample Contract Usage

```
contract CookieShop {  
    address owner;  
    mapping (address=>uint) public jar;  
  
    constructor() public {  
        owner = msg.sender;  
    }  
  
    function bake() public payable {  
        if(msg.value > 0.1 ether) {  
            jar[msg.sender] += 13;  
        }  
    }  
  
    function eat(uint count) public {  
        jar[msg.sender] -= count;  
    }  
  
    function close() public {  
        require(msg.sender == owner);  
        selfdestruct(msg.sender);  
    }  
}
```

bake() = 0xb0de262e

👤🚀 → bake() → ☐

👤🚀 → bake() → ☐

☐♂ → bake() → ☐

☐ owner: 👤 ☐👁

jar[☐♂] = 🍪 🍪

jar[👤🚀] = 🍪 🍪 🍪 🍪

Sample Contract Death

```
contract CookieShop {
  address owner;
  mapping (address=>uint) public jar;

  constructor() public {
    owner = msg.sender;
  }






  function bake() public payable {
    if(msg.value > 0.1 ether) {
      jar[msg.sender] += 13;
    }
  }


  function eat(uint count) public {
    jar[msg.sender] -= count;
  }

  function close() public {
    require(msg.sender == owner);
    selfdestruct(msg.sender);
  }
}
```

`close()` = 0x43d726d6

   → `close()` → 

 →  →   

 = 0x

`owner:[]`

`jar[]`

Geth and Parity Running Options

```
./geth --datadir  
/mnt/fastssd/.geth  
--rpc  
--rpcapi=debug,eth,net,rpc,web3  
--syncmode=full  
--gcmode=archive  
--cache 4096  
--trie-cache-gens 1024
```

```
parity -d /mnt/fastssd/.parity  
--jsonrpc-apis  
web3,eth,net,parity,rpc,traces  
--mode=active  
--pruning=archive  
--tracing=on --fat-db=on  
--min-peers=50 --max-peers=100  
--cache-size=4096  
--db-compaction=ssd  
--tx-queue-size=8192000  
--scale-verifiers --num-verifier  
--jsonrpc-server-threads 4  
--jsonrpc-threads 8
```

Archive Node Experience

archivedb assertion on when syncing and launch #9180



Closed computernity opened this issue on Jul 21 · 5 comments



computernity commented on Jul 21

Contributor



I'm running:

- Which Parity version?: 2.0.0 beta
- Which operating system?: Linux
- How installed?: binaries
- Are you fully synchronized?: no
- Which network are you connecting to?: mainnet
- Did you try to restart the node?: yes

I'm running parity with the following arguments:

```
./parity --no-ipc --pruning=archive --
```

debug.traceTransaction with reexec crashes #17431



Closed computernity opened this issue on Aug 17 · 2 comments



computernity commented on Aug 17



System information

Geth version: `geth version`

```
Version: 1.8.12-stable
Git Commit: 37685930d953bcbe023f9bc65b135a8d8b8f1488
Architecture: amd64
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.10.3
```

Hybrid Approach

Full Node + Etherscan API

<https://etherscan.io/apis>

- txlist
- txlistinternal

Latest 25 txns from a total Of 109 transactions

TxHash	Block	Age	From	
0x2fee0607ba1d19...	5216606	4 mins ago	0x7f720aa17df840f...	IN
0xade37816be1e00...	5216605	4 mins ago	0xc95bad7a549d3b...	IN
0x7b70ec86f9a49d...	5216605	4 mins ago	0xc95bad7a549d3b...	IN
0x361ce0cc65e399...	5216605	4 mins ago	0x097d2f2ffbf03e0b...	IN
0x1442ad578fec713...	5216602	5 mins ago	0x5b5b3e475501b6...	IN
0x0e23337e7d6d54...	5216602	5 mins ago	0xf898f063d22a994...	IN
0xb718b4fdbac8cb...	5216601	5 mins ago	0x327bfb6286026b...	IN

Contract Overview

ETH Balance:

0.16107 Ether

ETH USD Value:

\$119.64 (@ \$742.76/ETH)

No Of Transactions:

109 txns

Contract Source Code Verified

Contract Name:

KpopItem

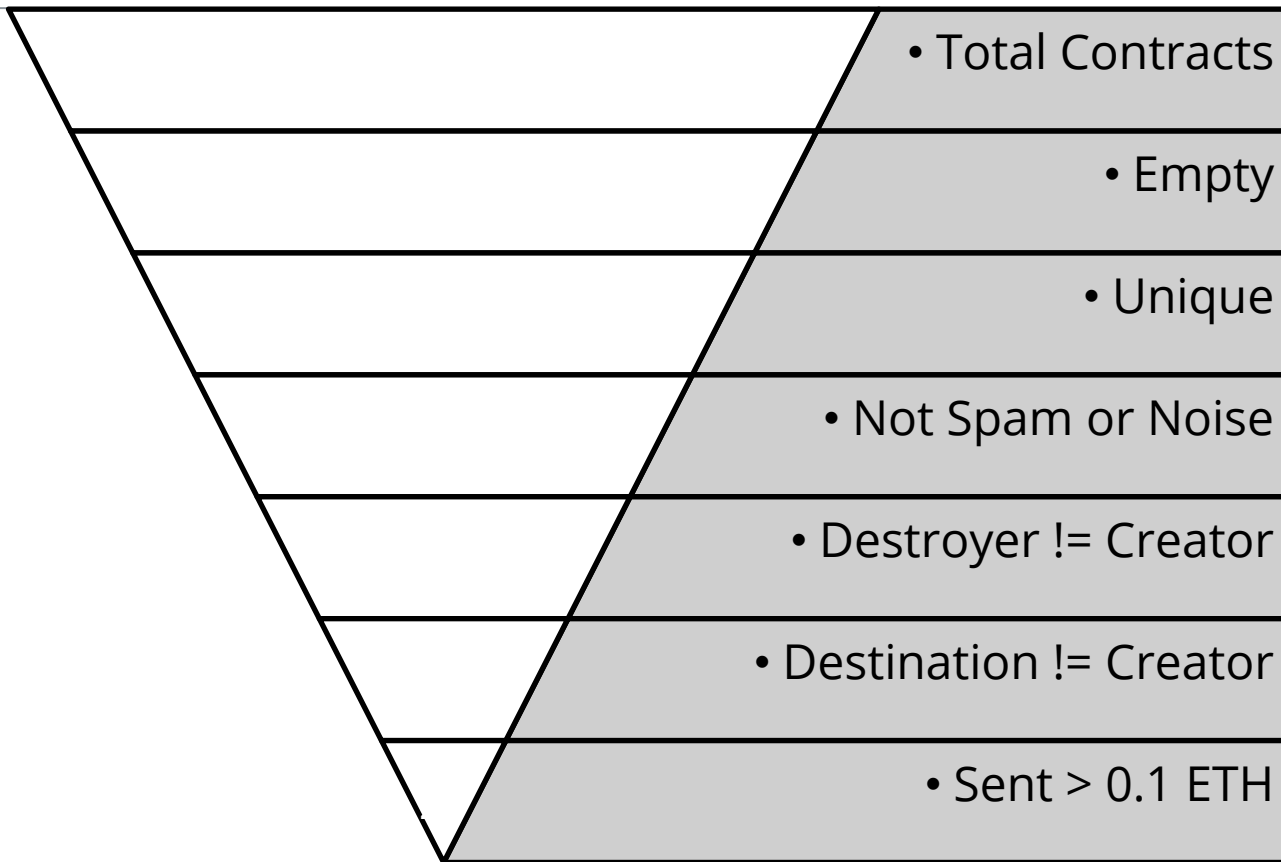
Compiler Version:

v0.4.20+commit.3155

Contract Source Code <>

```
1 // KpopItem is a ERC-721 item (https://gi
2 // Each KpopItem has its connected KpopTo
3 // Kpop.io is the official website
4
5 pragma solidity ^0.4.18;
6
7
8 /**
9  * @title SafeMath
10  * @dev Math operations with safety check
11  */
12 library SafeMath {
13
14     /**
15      * @dev Multiplies two numbers, throws o
16      */
17     function mul(uint256 a, uint256 b) inte
18         if (a == 0) {
19             return 0;
20         }
21         uint256 c = a * b;
```

Block 0 to 6,000,000 (July 20, 2018):

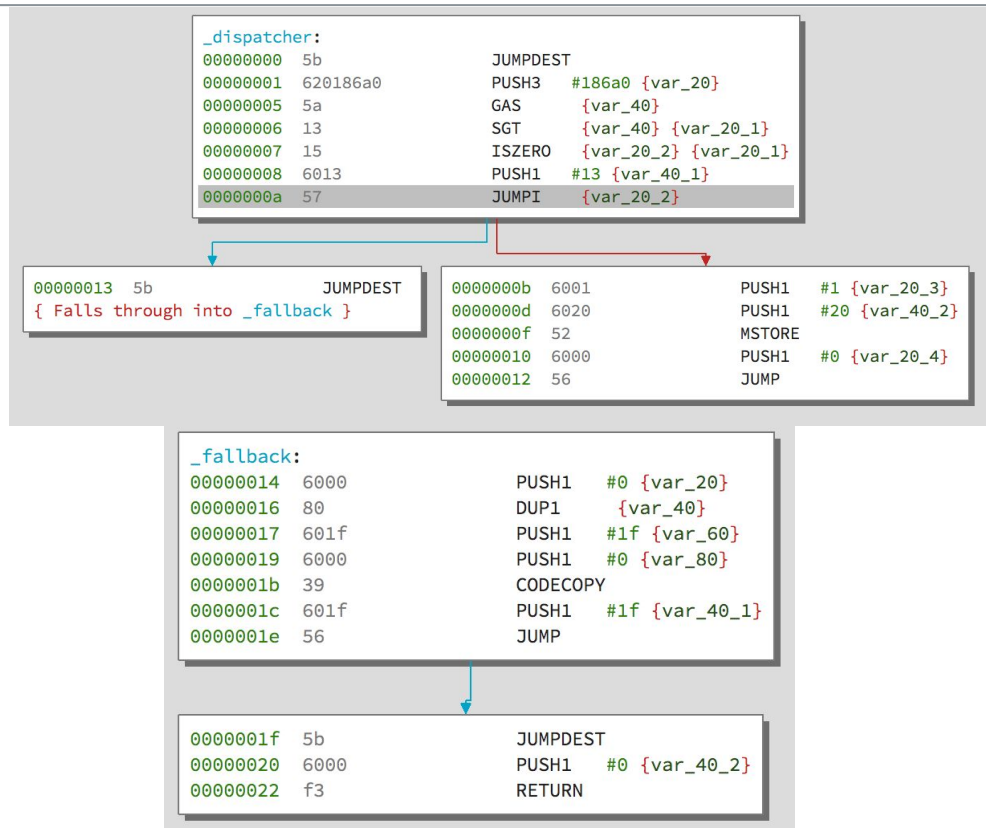


Top Duplicates

Count: 10,072

Code:

0x5b620186a05a1315
601357600160205260
00565b600080601f60
0039601f565b6000f3



Top Duplicates (2)

Count: 9,512

Code:

0x

Total: 6203 ETH

Top Duplicates (3)

Count: 1,963

Code:

[illegible]

6000 NULs (STOP)

***EIP-170 sets max size to 0x6000**

Noise / Spam

0x7F62E6C7Ec6700187aB99f71997912A9CDF184D1

PUSH20 0xff5932556071d5ac315d240b92b97a3b4f7daf3d
SELFDESTRUCT

0, 1 or 2 Wei transferred

~3,000 instances of this

Massive chained selfdestruct

<https://etherscan.io/tx/0x0bb3c5ec638d167a00d3e790cbf7692b39e70d343ad4900ef241c21e10d016a0>

0xd3e32594cedbc102d739142aa70d2114caea5618

Contract 0x0978b496a1635e4a0b4f867569cf43ee030e967 ⚠

Warning! Error encountered during contract execution (Out of gas) ⚠

SELF-DESTRUCT Contract 0x7fe8f3ab78407e54e19f9...

SELF-DESTRUCT Contract 0xfdd20f5050c96025a017...

SELF-DESTRUCT Contract 0xb7e2330fb74da72b66e0...

SELF-DESTRUCT Contract 0xd0273f27aa56cf7c178f...

SELF-DESTRUCT Contract 0xae0cc9e99b11cca9dc94...

SELF-DESTRUCT Contract 0xf30137e9ebd2ad27b8e8...

SELF-DESTRUCT Contract 0x4e01c88ee7766480a391...

SELF-DESTRUCT Contract 0x12ffc666a828961051e7...

SELF-DESTRUCT Contract 0x44aeb7d26a359d2e9c57...

SELF-DESTRUCT Contract 0x90f51a9a171a9b3ebc98...

SELF-DESTRUCT Contract 0x2b123d240f0eb64e95b...

SELF-DESTRUCT Contract 0x1d7019b512f9d3da284...

SELF-DESTRUCT Contract 0x69329f24e05ec98c81d...

SELF-DESTRUCT Contract 0x0b1c3cf74aaa0fe33683o...

SELF-DESTRUCT Contract 0x76139bee6a285e3b9f43...

SELF-DESTRUCT Contract 0x537ac90a527e87270554...

SELF-DESTRUCT Contract 0xd39ae24478b35b0d9b7...

SELF-DESTRUCT Contract 0x368b2efeca96542b30cc...

SELF-DESTRUCT Contract 0xc35481071fb2072e6abc...

SELF-DESTRUCT Contract 0xba1c2eb4d48a273394f1...

SELF-DESTRUCT Contract 0x429fb13d362de2d0957...

SELF-DESTRUCT Contract 0xf1b8a984b657ab3cea3e...

SELF-DESTRUCT Contract 0xc9f7bd19c4b8c1595e06...

SELF-DESTRUCT Contract 0xf3f9bd17b5c61db7c8b9...

SELF-DESTRUCT Contract 0x1c5c1595b0cf78464ddd...

SELF-DESTRUCT Contract 0xc0e5b4dc2ee26524dc8b...

SELF-DESTRUCT Contract 0xca9a97735557d7350b3...

SELF-DESTRUCT Contract 0x0fc67b4ce9b7ea2935d...

SELF-DESTRUCT Contract 0x8b2e079af6b3d0f6ee2...

SELF-DESTRUCT Contract 0x2839c0f4740906c4b366...

SELF-DESTRUCT Contract 0x42b43c236211bd8c58...

SELF-DESTRUCT Contract 0x1e24541018b45033cd5...

SELF-DESTRUCT Contract 0x8895e37a29993befab94...

SELF-DESTRUCT Contract 0xd3f83dc22b9883fa0e83...

SELF-DESTRUCT Contract 0x7233c01a6a2f0fa263c...

SELF-DESTRUCT Contract 0x21e24541018b45033cd5...

SELF-DESTRUCT Contract 0xf9950f5b302e69922dc1...

SELF-DESTRUCT Contract 0xd3d33cd8da3ca89ff8ed0...

SELF-DESTRUCT Contract 0xe2481cde2e5c6e999aa3...

SELF-DESTRUCT Contract 0x2e158e3256225a0f299e...

SELF-DESTRUCT Contract 0xda5846baa1bde1ad5f1...

SELF-DESTRUCT Contract 0xb87dbb5f6a147d9a4cf...

SELF-DESTRUCT Contract 0x9d688e06b12b482b8be...

SELF-DESTRUCT Contract 0xe01032a6a363ebc0f0c...

SELF-DESTRUCT Contract 0x299e0d8ebfbab5cf3e5e...

SELF-DESTRUCT Contract 0x5a2a894c5a7128b95d...

SELF-DESTRUCT Contract 0x42721d2498de037ec19...

SELF-DESTRUCT Contract 0xb32988b23023551e350f...

SELF-DESTRUCT Contract 0x3ce1a6b2bec7ae018fe8...

SELF-DESTRUCT Contract 0xa0cb84d8093d12d8f815...

SELF-DESTRUCT Contract 0x055c74de2af7177c8c33...

SELF-DESTRUCT Contract 0x4e7c1c91218cf753a038...

SELF-DESTRUCT Contract 0xfcaa1606be362c02864...

SELF-DESTRUCT Contract 0x9a310671bb1795127aec...

SELF-DESTRUCT Contract 0x8c3f48dd581df0080f8c...

SELF-DESTRUCT Contract 0xed0e20756a38aa168b3...

SELF-DESTRUCT Contract 0x4ad9a80d8c2e6a27ad42...

SELF-DESTRUCT Contract 0x74688a137d790d58e04...

SELF-DESTRUCT Contract 0x7d54e2c5ce75f147d7d...

SELF-DESTRUCT Contract 0xd43dd3c2aff1ac8697d0...

SELF-DESTRUCT Contract 0xd6a25ab326472a0662d...

SELF-DESTRUCT Contract 0xd595358e5bce12e871c3...

SELF-DESTRUCT Contract 0x3ce7d495dcdfcfc129e5...

SELF-DESTRUCT Contract 0xa08967e66d20e3e696cb...

SELF-DESTRUCT Contract 0xeb4460d93e2f0ca2f84b...

SELF-DESTRUCT Contract 0x7cbe89d944e90c6ac554...

SELF-DESTRUCT Contract 0x5be894573dc43cb032...

SELF-DESTRUCT Contract 0x88ce6b713bc5a07b943...

SELF-DESTRUCT Contract 0x2f39d3f2f03a1e26229b...

SELF-DESTRUCT Contract 0x7151cbe210a214faee22...

SELF-DESTRUCT Contract 0x8f3d61d394882039174...

SELF-DESTRUCT Contract 0x4a47a539e434af31e42...

SELF-DESTRUCT Contract 0x79a8c8ca9304dd432795...

SELF-DESTRUCT Contract 0x6662d4a436c5251f90e6...

SELF-DESTRUCT Contract 0x724366ca20662edb806...

SELF-DESTRUCT Contract 0x4fa0ab11c9c03bcc31a0...

SELF-DESTRUCT Contract 0xb42dec2a3a6683edd29...

SELF-DESTRUCT Contract 0x1e998271761742dcd0...

SELF-DESTRUCT Contract 0x48e50cf4f41b0dc028db...

SELF-DESTRUCT Contract 0x45b0f65639651827ab46...

SELF-DESTRUCT Contract 0x2bc03999055803d99f6f...

SELF-DESTRUCT Contract 0x1e9845db13ca712cb1...

SELF-DESTRUCT Contract 0x94e70bcf859eb39a2dc7...

SELF-DESTRUCT Contract 0xcdf5ba2fd27350f17d267e...

SELF-DESTRUCT Contract 0x0c0da94b729a33a467...

SELF-DESTRUCT Contract 0x4a6155fcb3b13fa3584...

SELF-DESTRUCT Contract 0x55fc93872ec69f2a2149...

SELF-DESTRUCT Contract 0xd8bb5e0c68f50c8662c2...

SELF-DESTRUCT Contract 0x3be51b159ec8d3732e41...

SELF-DESTRUCT Contract 0xb6b6ce2bf32baca0ad...

SELF-DESTRUCT Contract 0x152e020dbc7b7866248...

SELF-DESTRUCT Contract 0xb55e5d969a126a4b74ab...

SELF-DESTRUCT Contract 0x200537ec30f9d7fca0cd5...

SELF-DESTRUCT Contract 0x3f94995a02f67edd44fc7...

SELF-DESTRUCT Contract 0xb4eaf6c2b126f1fec329...

SELF-DESTRUCT Contract 0x7c3477e53f1ca0bc33e...

SELF-DESTRUCT Contract 0x1e92562a6b0cb95a9c0a...

SELF-DESTRUCT Contract 0x6f67564fde675da2cad6...

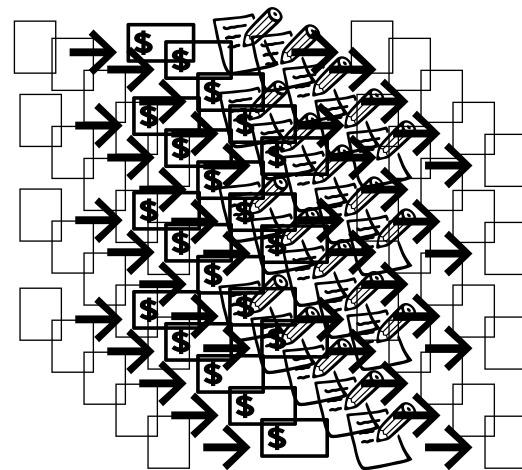
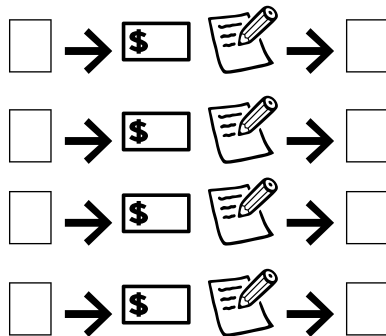
SELF-DESTRUCT Contract 0x7226989ecd32decca7d...

SELF-DESTRUCT Contract 0x03234b831a6a3c402ae...

SELF-DESTRUCT Contract 0x269be445456ec458a8c...

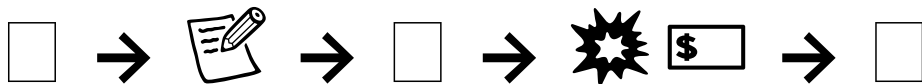
SELF-DESTRUCT Contract 0x08ba6d6004d961d688fa...

Massive selfdestruct

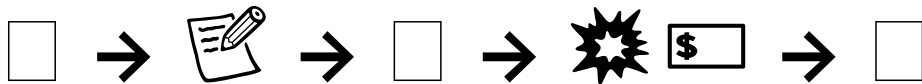


2000

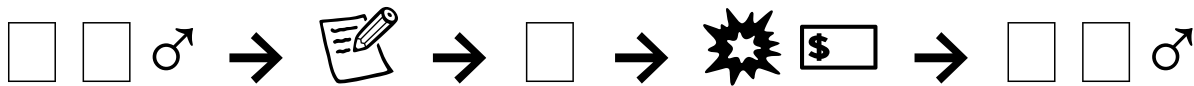
2000



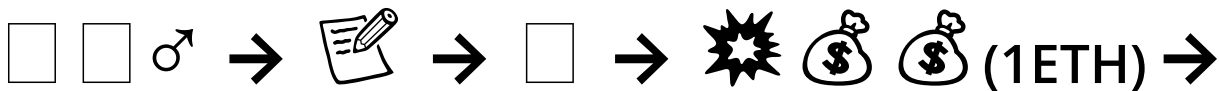
630



160



16



□ □ ♂

50ETH to 0x0

0xf73d247ffDBD5A9964d1a1444c86343650b67ed4

<https://etherscan.io/address/0xf73d247ffdbd5a9964d1a1444c86343650b67ed4>

c86343650b67ed4

Function: kill(address _to) MethodID: 0xcbf0b0c0

[0] :

[illegible]

300ETH selfdestruct

Account:0x96f65700904cB464F3D153a2744B84FCa27ABF9C

Sent 300ETH to 0xCafe00be401442Bfb5E480C355393FD8C147abBB

```
Function: changeOwner(address _from, address _to) ***
```

MethodID: 0xf00d4b5d

[illegible][illegible]

Dice2Win

0xD1CEee6B94DE402e14F24De0871580917ede8a7

Sent 65.7 ETH to 0xD1CEee271fD5a8B0e2BFc12Ea5B5b2E5CeDEc95

Function: `approveNextOwner(address _nextOwner)`

MethodID: 0xd579fd44

[illegible]

Etherwow

0x4DF6DE08D11f11EBAd5d9E136B768849426fB8a7

Function: ownerChangeOwner(address newOwner)

MethodID: 0x4f44728d

[0]: 000000000000000000000000000000007d138be0eed529ae42a468472b2beb0314af5e28

Function: ownerkill()

```
/** @dev owner selfdestruct contract
***BE CAREFUL! EMERGENCY ONLY
/ CONTRACT UPGRADE*** */
function ownerkill() publiconlyOwner
{ selfdestruct(owner); }
```

Etherwow

国内最火爆的区块链猜数字小游戏

选择投注类型

数字

76

51

31

16

代币

0.1

0.2

1

0.5

赢币

0.12

0.36

3

3

The most popular blockchain guessing digital game in China

.2 ETH

0xcd6d2cd79fd754c6b909585e46541d32ec491962

0x00bb585e7be7b095be9aba3c5777121c5ba7924a:
: Adds 0.2 Ether

0x3f9ed84ef180fae940ebf4bce4c4d70e2f751482:
: **0xa840dda9**

0x3f9ed84ef180fae940ebf4bce4c4d70e2f751482:
: **kill()**
=> selfdestruct

0x3f9ed84ef180fae940ebf4bce4c4d70e2f751482

Becoming Mortal for 3ETH

0xf4D3CEd0929eA3F3Fd94F32ba460a66b428932F2

```
function mortal() { owner = msg.sender; }  
function kill() {  
    if(msg.sender == owner) selfdestruct(owner);  
}
```

Conclusion

Analysis possible but takes patience

- Only 16 of 32,000 contracts sent >1 ETH to address != original creator
- Few doing this analyze without etherscan making analysis centralized

Next Steps

- Analyze TX before selfdestruct
- Internal transactions need to be made more accessible

Contact

Jay Little, Principal Security Engineer

jay@trailofbits.com

@computerality

@trailofbits

www.trailofbits.com

github.com/trailofbits

blog.trailofbits.com

Use our Tools

Rigorously test, assess, and understand your contracts with Slither, Manticore, and Echidna

Accounts and Transactions and Blocks



- Account: ☐
- Contract: ☐
- 1 Ether (ETH) = 10^{18} Wei
- 21000 Wei per TX
- Contracts can call other contracts

