



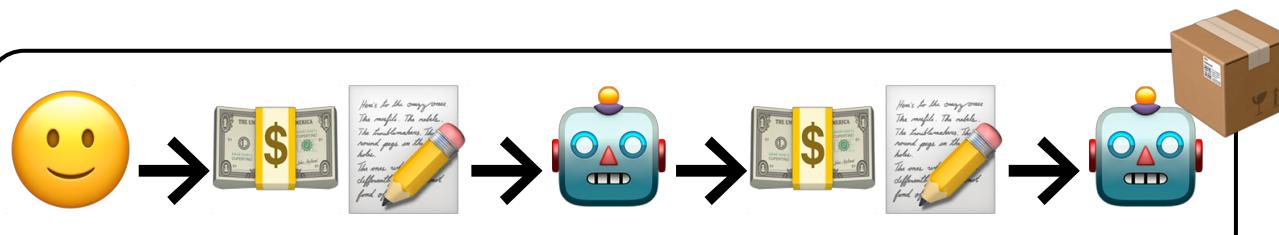
Blockchain Autopsies: Analyzing selfdestructs

Jay Little
devcon4
November 1, 2018

Accounts and Transactions and Blocks



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



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

chef → **close()** → robot

robot → money → chef

robot = 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** computerality opened this issue on Jul 21 · 5 comments



computerality 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 connected 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** computerality opened this issue on Aug 17 · 2 comments



computerality 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

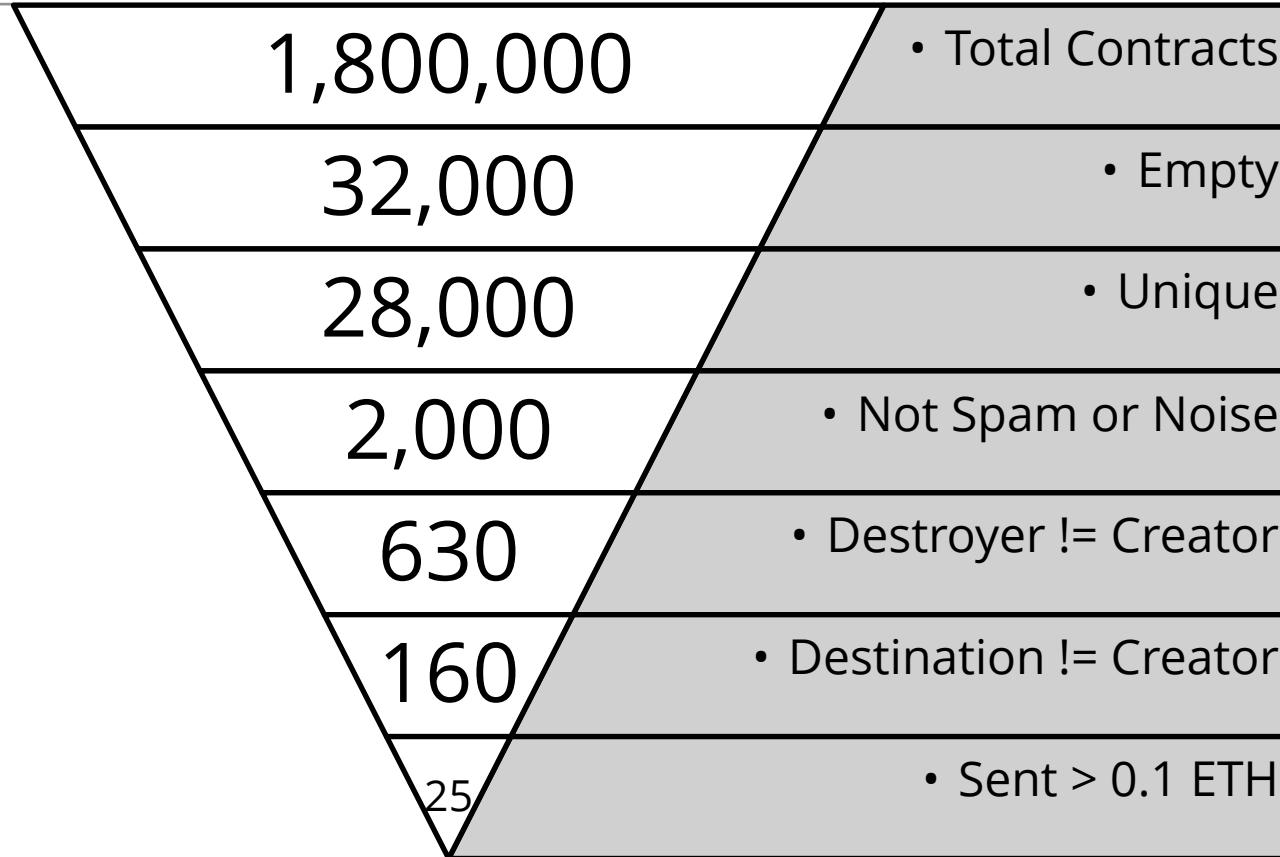
Latest 25 txns from a total Of 109 transactions				
TxHash	Block	Age	From	To
0x2fee0607ba1d19...	5216606	4 mins ago	0x7f720aa17df840f...	IN
0xade37816be1e00...	5216605	4 mins ago	0xc95bad7a549d3b...	IN
0x7b70ec86f9a49d...	5216605	4 mins ago	0xc95bad7a549d3b...	IN
0x361ce0cc65e399...	5216605	4 mins ago	0x097d2ffbf03e0b...	IN
0x1442ad578fec713...	5216602	5 mins ago	0x5b5b3e475501b6...	IN
0xe0e23337e7d6d54...	5216602	5 mins ago	0xf898f063d22a994...	IN
0xb718b4fdbac8cb...	5216601	5 mins ago	0x327fbf6286026b...	IN

Contract Overview	
ETH Balance:	0.16107 Ether
ETH USD Value:	\$119.64 (@ \$742.76/ETH)
No Of Transactions:	109 txns

Contract Name: KpopItem
Compiler Version: v0.4.20+commit.3155
Contract Source Code Verified

```
Contract Source Code </>
1 // KpopItem is a ERC-721 item (https://github.com/Kpopio/KpopItem)
2 // Each KpopItem has its connected KpopToken
3 // Kpop.io is the official website
4
5 pragma solidity ^0.4.18;
6
7 /**
8  * @title SafeMath
9  * @dev Math operations with safety checks
10 */
11
12 library SafeMath {
13
14 /**
15  * @dev Multiplies two numbers, throws on overflow.
16  */
17 function mul(uint256 a, uint256 b) internal pure returns (uint256) {
18     if (a == 0) {
19         return 0;
20     }
21     uint256 c = a * b;
22     require(c / a == b);
23     return c;
24 }
```

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:

```
0x00000000000000000000000000000000000000000000000000000000000000  
00000000000000000000...00000000000000000000000000000000
```

6000 NULs (ST0P)

*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>

0xd3e32594cedbc102d739142aa70d21f4caeae5618

Q Contract 0x0978b496a1635e4a0b4ff867569cf43ee030e967 ▲

Warning! Error encountered during contract execution [Out of gas] ☹

SELF-DESTRUCT Contract 0x7fe6f3ab78407e54e19f9...

SELF-DESTRUCT Contract 0xfd202f5050c98025a017...

SELF-DESTRUCT Contract 0xb7e2330fb72da72b66e0...

SELF-DESTRUCT Contract 0xd0273f27aa56fcf7c178f...

SELF-DESTRUCT Contract 0xaebcc9e99b11cca9dc94...

SELF-DESTRUCT Contract 0xf30137e9ebd2ad27b7b68...

SELF-DESTRUCT Contract 0x4e01c8ee7766480e391...

SELF-DESTRUCT Contract 0x12cff668a28961051e7...

SELF-DESTRUCT Contract 0x44eb72d5e8659d2e9c54...

SELF-DESTRUCT Contract 0x90f51a9a171b3ebc98...

SELF-DESTRUCT Contract 0x2b123e2d4f0ebf94e95b...

SELF-DESTRUCT Contract 0x1d7019b512f0e93da284...

SELF-DESTRUCT Contract 0x69329f24e05ec98c61d...

SELF-DESTRUCT Contract 0x0b1c3cf74aaa0fe33863c...

SELF-DESTRUCT Contract 0x7619bbe628563bf043...

SELF-DESTRUCT Contract 0x537ac00a527e87270554...

SELF-DESTRUCT Contract 0xd39ae24478b35b0d9b7...

SELF-DESTRUCT Contract 0x368b2fecfa96542b30cc...

SELF-DESTRUCT Contract 0xc35481071fb2072e6abc...

SELF-DESTRUCT Contract 0xba1c2eb4d48a273394f1...

SELF-DESTRUCT Contract 0x429fb13d3262de2d9057...

SELF-DESTRUCT Contract 0xfb8ba984b657ab3cea3e...

SELF-DESTRUCT Contract 0xcf97bd19c4b8c1595c68...

SELF-DESTRUCT Contract 0x3f90bd17b561d67b69...

SELF-DESTRUCT Contract 0x1c51c595bcf7e6484ddd...

SELF-DESTRUCT Contract 0xce5b4ddc2ee28524d8b...

SELF-DESTRUCT Contract 0xca9a097735557d7350b3...

SELF-DESTRUCT Contract 0x0fc67b4f4ce0bf7ea2935d...

SELF-DESTRUCT Contract 0xb8b2f079a6fb93d0fce2...

SELF-DESTRUCT Contract 0x2839c0f4740906b4c368...

SELF-DESTRUCT Contract 0x42b43c23621bdc6c58...

SELF-DESTRUCT Contract 0x1b2454101B945033cd5...

SELF-DESTRUCT Contract 0x8895e37a29993befab94...

SELF-DESTRUCT Contract 0xd3f83dc22b9883fa0e83...

SELF-DESTRUCT Contract 0x7233c01a6a20fefa263c...

SELF-DESTRUCT Contract 0xb3e738f9201122a734b...

SELF-DESTRUCT Contract 0x9950f5b302e69922d1...

SELF-DESTRUCT Contract 0xddb33cda93a89ffedf0...

SELF-DESTRUCT Contract 0x2481c01e05c5c99aa3...

SELF-DESTRUCT Contract 0x2e158e3256225a0f298e...

SELF-DESTRUCT Contract 0xda5846bea1bded1ad51...

SELF-DESTRUCT Contract 0xb7dbb5f6a147d9a4acf...

SELF-DESTRUCT Contract 0x9d88e0612b482b8b...

SELF-DESTRUCT Contract 0xe01032a8a363ebcc0fce...

SELF-DESTRUCT Contract 0x299e0de8fbaf5c3e5...

SELF-DESTRUCT Contract 0x5a26a884c5a7128b055d...

SELF-DESTRUCT Contract 0x42721d2498de037ec19...

SELF-DESTRUCT Contract 0xb2968b23023551e950f...

SELF-DESTRUCT Contract 0x19132313e5468ac55ce0...

SELF-DESTRUCT Contract 0x6ae10ecd00dc36a86bf...

SELF-DESTRUCT Contract 0x322f611499362975h0...

SELF-DESTRUCT Contract 0x3ce1a6b2bec7ae01f8e8...

SELF-DESTRUCT Contract 0xa0cb84d8003d12d8f815...

SELF-DESTRUCT Contract 0x0557c4d2a77177e835...

SELF-DESTRUCT Contract 0x4e7c1c91218f7c753a038...

SELF-DESTRUCT Contract 0xcaa1406b6e362c02864...

SELF-DESTRUCT Contract 0x9a310671bb795127aec...

SELF-DESTRUCT Contract 0x8c48dd5f10080fbc...

SELF-DESTRUCT Contract 0xed020756a3cae168b3...

SELF-DESTRUCT Contract 0x4ad9a80d8c2e62a7ad42...

SELF-DESTRUCT Contract 0x74688a137679d058a04...

SELF-DESTRUCT Contract 0x7d54e2c5c5a76f147d7d...

SELF-DESTRUCT Contract 0x4d9dd3c2a1f1c6897d0...

SELF-DESTRUCT Contract 0x6a25ab326472a0682...

SELF-DESTRUCT Contract 0xd595356b5cbe12e71c3...

SELF-DESTRUCT Contract 0x8ec7d495dcdff128e5...

SELF-DESTRUCT Contract 0xa08967e5b2d2ce3590cb...

SELF-DESTRUCT Contract 0x4eb4d3c9a2f0c21b4...

SELF-DESTRUCT Contract 0x7cbe6944e900c6a654...

SELF-DESTRUCT Contract 0x5be8394573dc43cb032...

SELF-DESTRUCT Contract 0x88ca6e713bc5a7b943...

SELF-DESTRUCT Contract 0x2ff93d2f03a1e26229b...

SELF-DESTRUCT Contract 0x7151cbe210a214fae22...

SELF-DESTRUCT Contract 0x8f3d613949820399174...

SELF-DESTRUCT Contract 0x4a7a59e434fd13e42...

SELF-DESTRUCT Contract 0x79a8c6a304d423795...

SELF-DESTRUCT Contract 0x6682d4a36c251906...

SELF-DESTRUCT Contract 0x224a6e7c90470c8aa04...

SELF-DESTRUCT Contract 0x99dc4b4d6a3b1a12d...

SELF-DESTRUCT Contract 0x83a599c095dca615cf...

SELF-DESTRUCT Contract 0x6ae10ecd00dc36a86bf...

SELF-DESTRUCT Contract 0x322f611499362975h0...

SELF-DESTRUCT Contract 0x299e0de8fbaf5c3e5...

SELF-DESTRUCT Contract 0x1e92562a8c625195a9c0a...

SELF-DESTRUCT Contract 0x7f641d8e75da2cad8...

SELF-DESTRUCT Contract 0x7226098ec032deca7d...

SELF-DESTRUCT Contract 0x03f234b831a6a3c402ae...

SELF-DESTRUCT Contract 0x269be445456ec5458a8c...

SELF-DESTRUCT Contract 0x08ba6d8004961d688fa...

SELF-DESTRUCT Contract 0x724366ca2068c2edb806...

SELF-DESTRUCT Contract 0x4fa0ab11c9c03bcc31a0...

SELF-DESTRUCT Contract 0xb42dec2a3a6683ed29...

SELF-DESTRUCT Contract 0x1e938271761742dedf0...

SELF-DESTRUCT Contract 0x48e50cf4f41b0dc028d...

SELF-DESTRUCT Contract 0x45b0f65639651872ab46...

SELF-DESTRUCT Contract 0x2bc03999055803d99f6...

SELF-DESTRUCT Contract 0x1e9845db13ca712c1...

SELF-DESTRUCT Contract 0x94e70bcf859eb39a2dc7...

SELF-DESTRUCT Contract 0xcf5ba2f2d7350f17d267e...

SELF-DESTRUCT Contract 0xdfc00da94fb29a33a467...

SELF-DESTRUCT Contract 0x4fa155fcbe13bfa3584...

SELF-DESTRUCT Contract 0x55f93872c69f2a24149...

SELF-DESTRUCT Contract 0x6bb5e0c68f50d28662c...

SELF-DESTRUCT Contract 0x3be151b9ec83d732e41...

SELF-DESTRUCT Contract 0x6be5c834d997e205053...

SELF-DESTRUCT Contract 0xbb6face2bf32baca0ad...

SELF-DESTRUCT Contract 0x152a020db2c7b7896248...

SELF-DESTRUCT Contract 0xbb5d969a126a4b74ab...

SELF-DESTRUCT Contract 0x200537ec0f9d7fca0dc5...

SELF-DESTRUCT Contract 0x3f949950a0f76f7dd4cf7...

SELF-DESTRUCT Contract 0xba4ec62b1b26f1e329...

SELF-DESTRUCT Contract 0x7c3477e5f341cabcc33e...

SELF-DESTRUCT Contract 0x1e92562a8c625195a9c0a...

SELF-DESTRUCT Contract 0x7f641d8e75da2cad8...

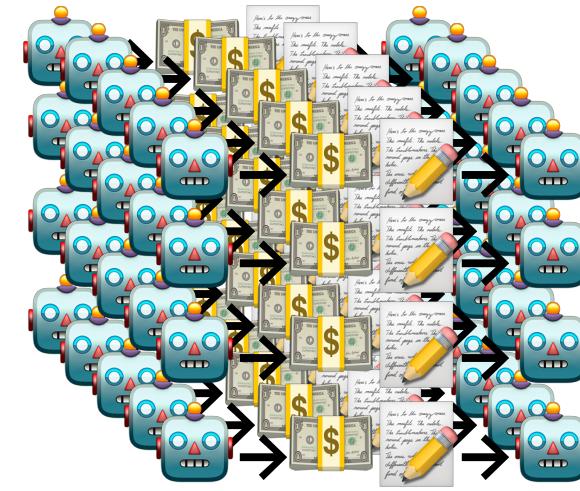
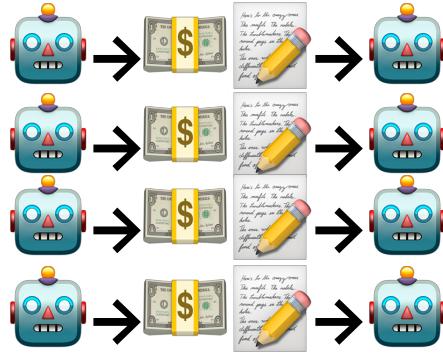
SELF-DESTRUCT Contract 0x7226098ec032deca7d...

SELF-DESTRUCT Contract 0x03f234b831a6a3c402ae...

SELF-DESTRUCT Contract 0x269be445456ec5458a8c...

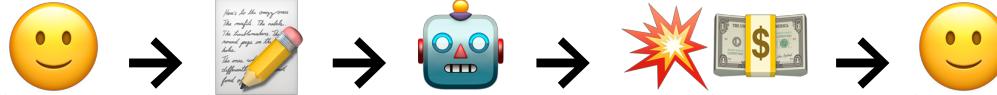
SELF-DESTRUCT Contract 0x08ba6d8004961d688fa...

Massive selfdestruct

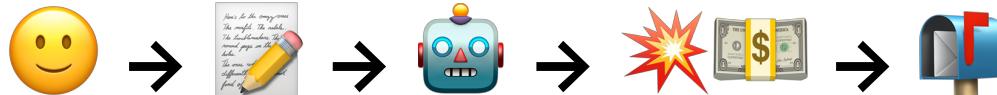


2000

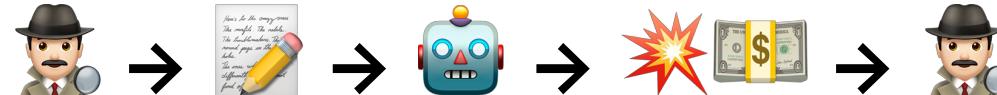
2000



630



160



16



50ETH to OXO

0xf73d247ffDBD5A9964d1a1444c86343650b67ed4

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

Function: kill(address _to) MethodID: 0xcbf0b0c0

[θ] :

300ETH selfdestruct

Account: 0x96f65700904cB464F3D153a2744B84FCa27ABF9C

Sent 300ETH to 0xCafe00be401442Bfb5E480C355393FD8C147abBB

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

MethodID: 0xf00d4b5d

```
[1]: 00000000000000000000000000000000afe00be401442bfb5e480c355393fd8c147abbb
```

Dice2Win

0xD1CEeee6B94DE402e14F24De0871580917ede8a7

Sent 65.7 ETH to 0xD1CEeee271fd5a8B0e2BFc12Ea5B5b2E5CeDEC95

Function: approveNextOwner(address _nextOwner)

MethodID: 0xd579fd44

[0]: 000000000000000000000000d1ceeee271fd5a8b0e2bfcc12ea5b5b2e5cedec95

Etherwow

0x4DF6DE08D11f11EBAd5d9E136B768849426fB8a7

Function: ownerChangeOwner(address newOwner)

MethodID: 0x4f44728d

[0]: 000000000000000000000000000000007d138be0eed529ae42a468472b2beb0314af5e28

Function: ownerkill()

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

投币

0.1

赢币

0.12

51

0.2

0.36

31

1

3

16

0.5

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