Blockchain Autopsies: Analyzing selfdestructs

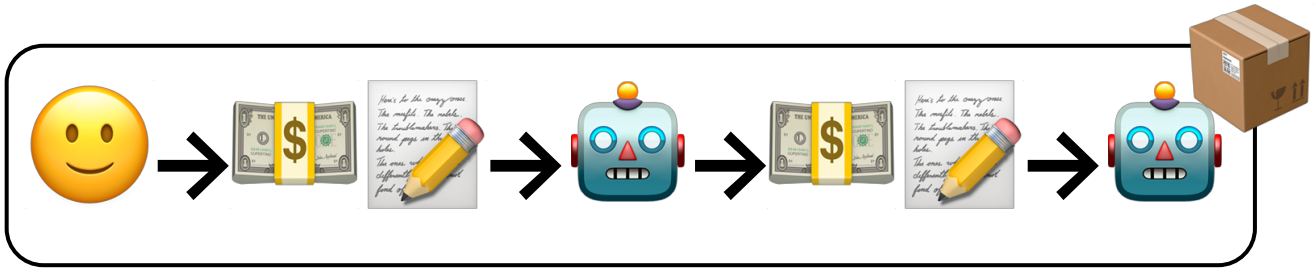
Jay Little

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

👨‍🍳 → close() → 🤖

🤖 → 💵 → 👨‍🍳

🤖 = 0x

owner:[]

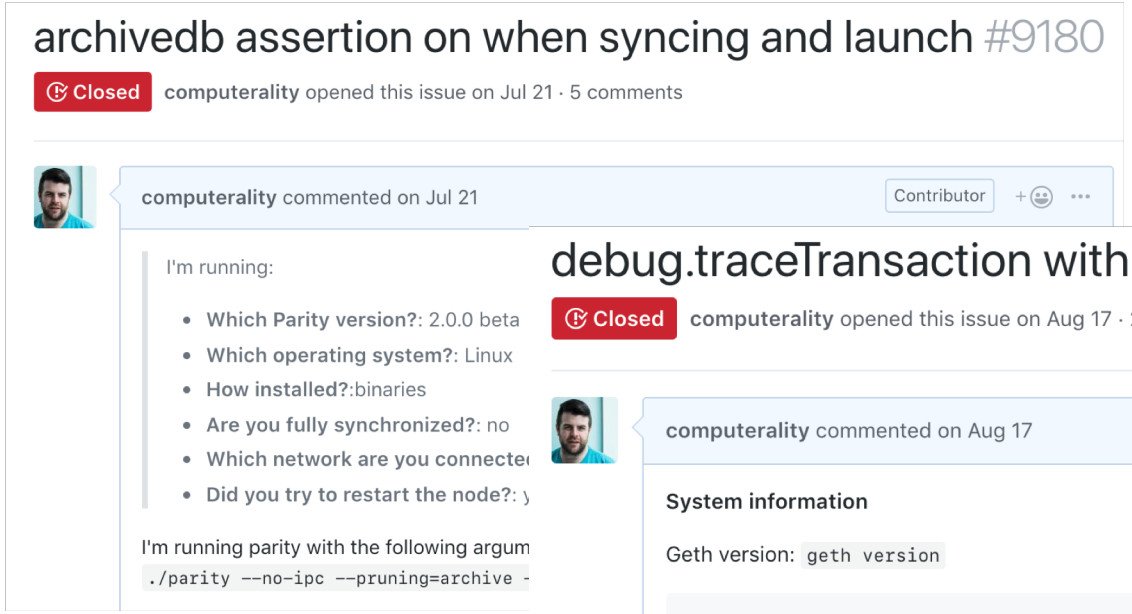
jar[]

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

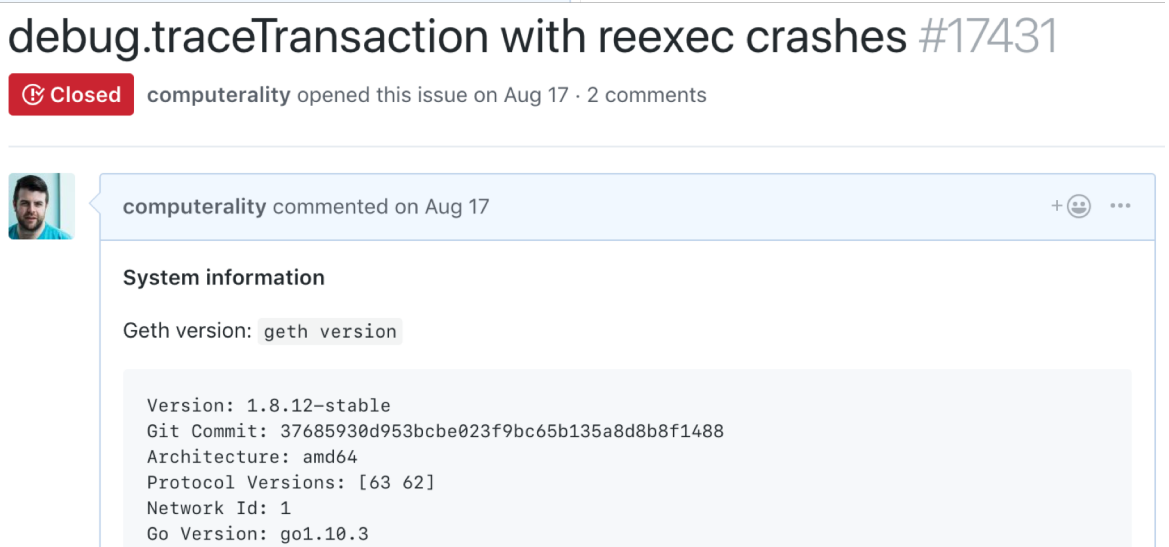
computerality commented on Jul 21 — Contributor

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 connecte**
- **Did you try to restart the node?**: y

I'm running parity with the following argum

```
./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`

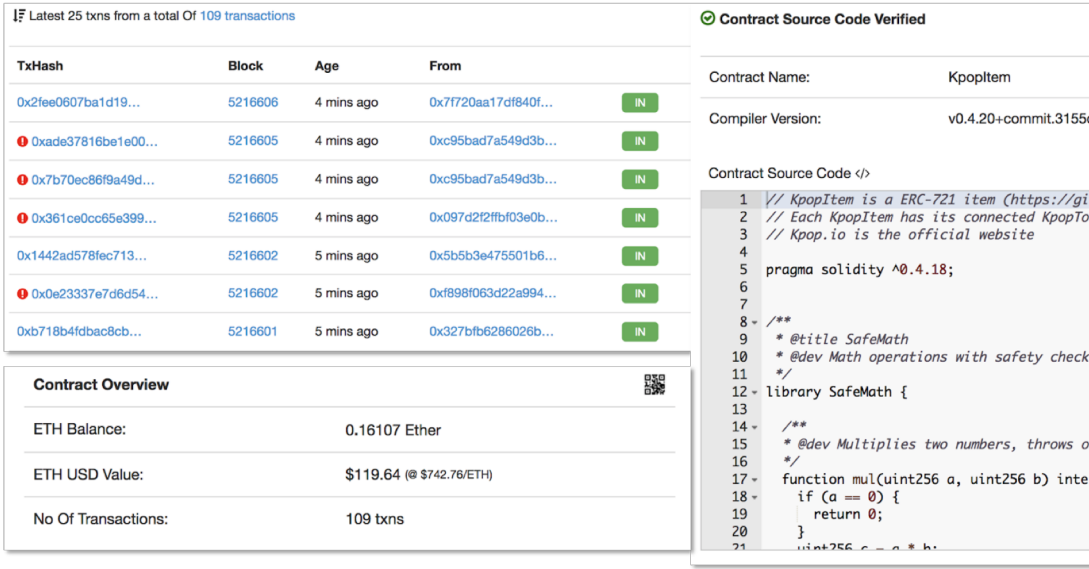
```
Version: 1.8.12-stable
Git Commit: 37685930d953bcbe023f9bc65b135a8d8b8f1488
Architecture: amd64
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.10.3
```

Hybrid Approach

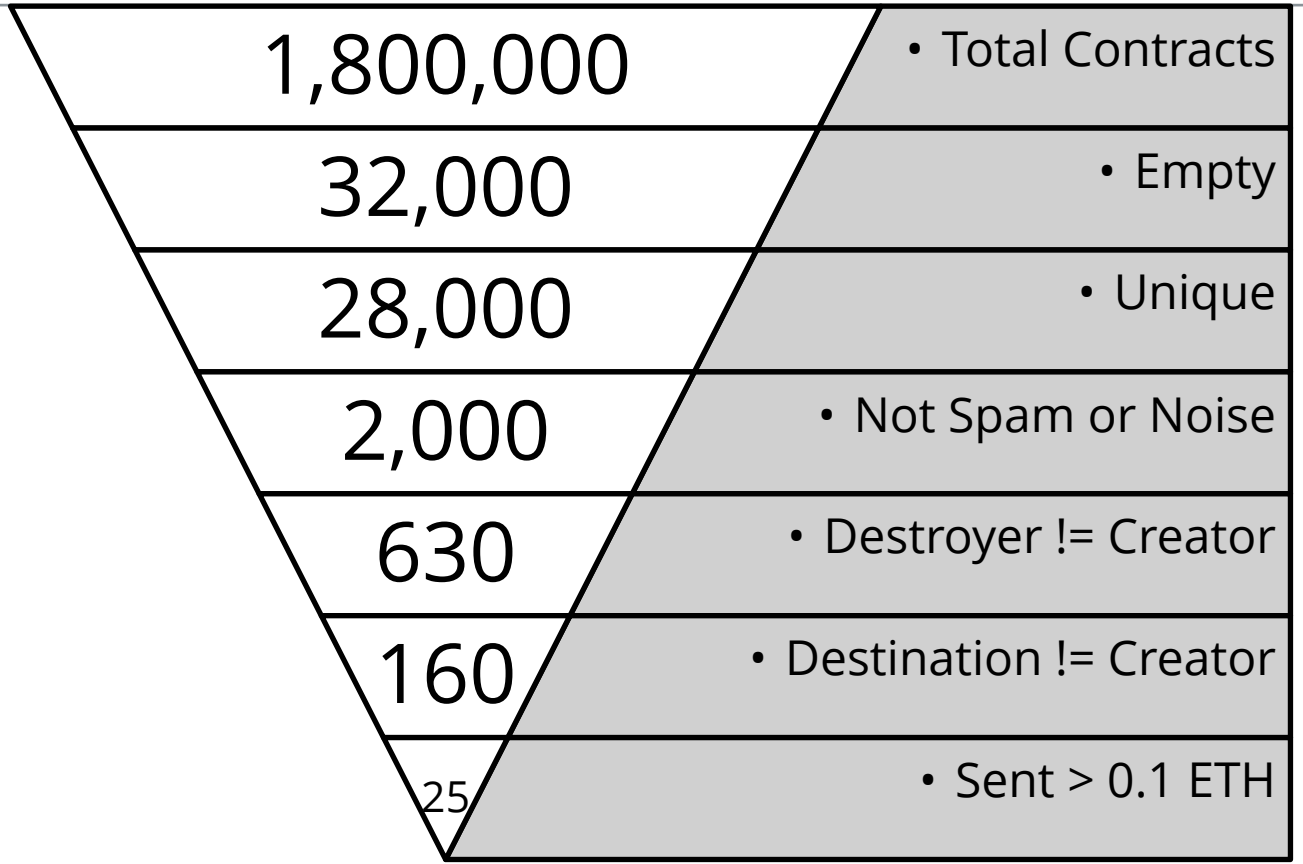
Full Node + Etherscan API

https://etherscan.io/apis

- txlist
- txlistinternal



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



Top Duplicates

Count: 10,072

Code:

```
0x5b620186a05a1315
60135760016020526 0
00565b600080601f60
0039601f565b6000f3
```

Top Duplicates (2)

Count: 9,512

Code:

```
0x
```

Total: 6203 ETH

Top Duplicates (3)

Count: 1,963

Code:

```
0x0000000000000000000000000000000000000000000000000000000000000000…0000000000000000000000
```

6000 NULs (STOP)

*EIP-170 sets max size to 0x6000

Noise / Spam

0x7F62E6C7Ec6700187aB99f71997912A9CDF184D1

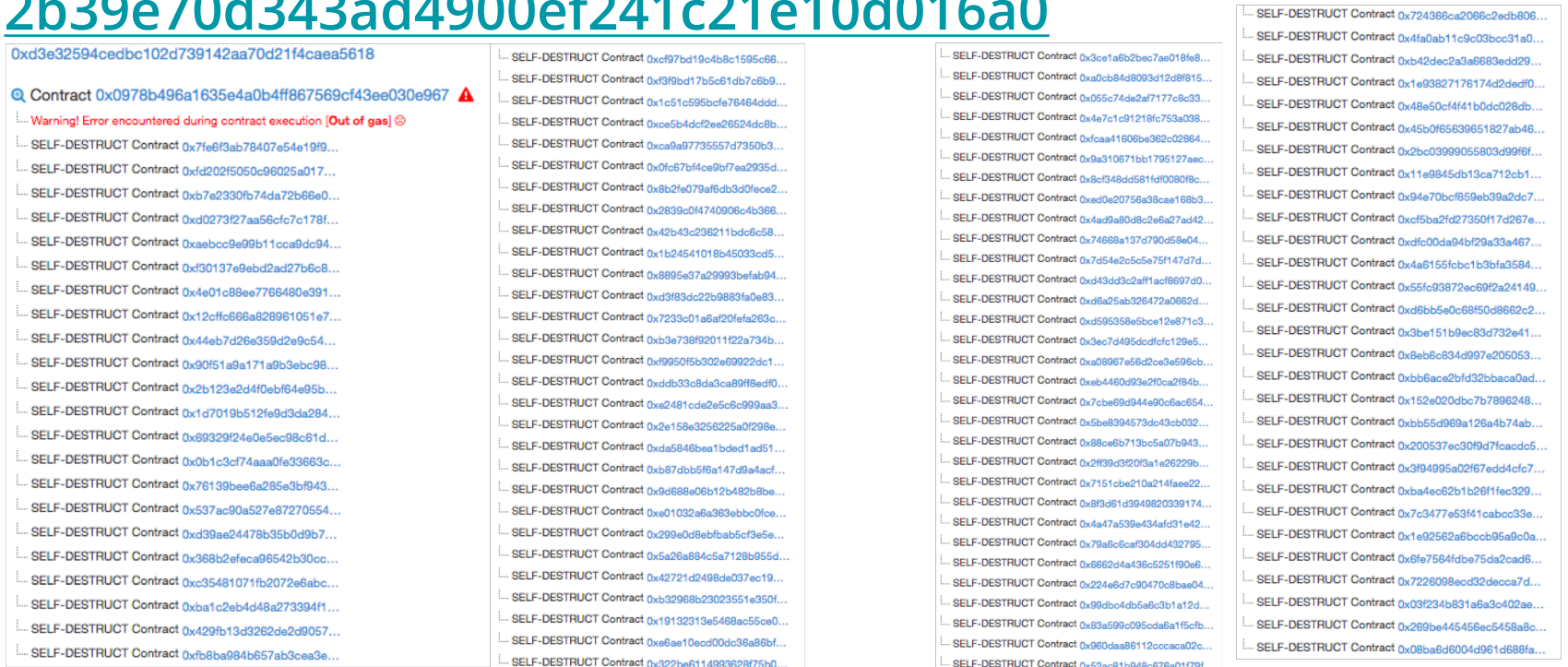
```
PUSH20 0xff5932556071d5ac315d240b92b97a3b4f7daf3d
SELFDESTRUCT
```

0, 1 or 2 Wei transferred

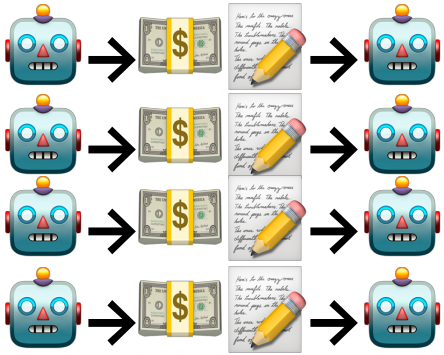
~3,000 instances of this

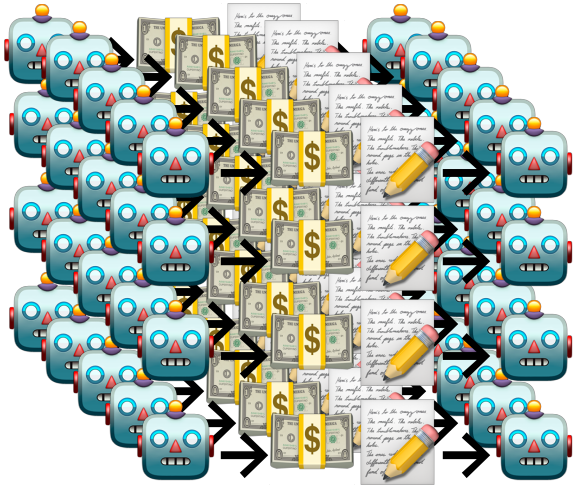
Massive chained selfdestruct

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



Massive selfdestruct





2000

2000 🙂 →  → 🤖 → 💥💵 → 🙂

630 🙂 →  → 🤖 → 💥💵 → 📪

160 🕵️ →  → 🤖 → 💥💵 → 🕵️

16 🕵️ →  → 🤖 → 💥💰💰 (1ETH) → 🕵️

50ETH to 0x0

0xf73d247ffDBD5A9964d1a1444c86343650b67ed4

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

```
Function: kill(address _to) MethodID: 0xcbf0b0c0

[0]:
0000000000000000000000000000000000000000000000000000000000000000
```

300ETH selfdestruct

```
Account:0x96f65700904cB464F3D153a2744B84FCa27ABF9C

Sent 300ETH to 0xCafe00be401442Bfb5E480C355393FD8C147abBB


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

MethodID: 0xf00d4b5d

[0]:  000000000000000000000000374139a05ac55917badd3f934f1b93f5c8623ded

[1]:  000000000000000000000000cafe00be401442bfb5e480c355393fd8c147abbb
```

Dice2Win

0xD1CEeee6B94DE402e14F24De0871580917ede8a7

Sent 65.7 ETH to 0xD1CEeee271fD5a8B0e2BFc12Ea5B5b2E5CeDEc95

Function: approveNextOwner(address _nextOwner)

MethodID: 0xd579fd44

[0]: 000000000000000000000000d1ceeee271fd5a8b0e2bfc12ea5b5b2e5cedec95

Etherwow

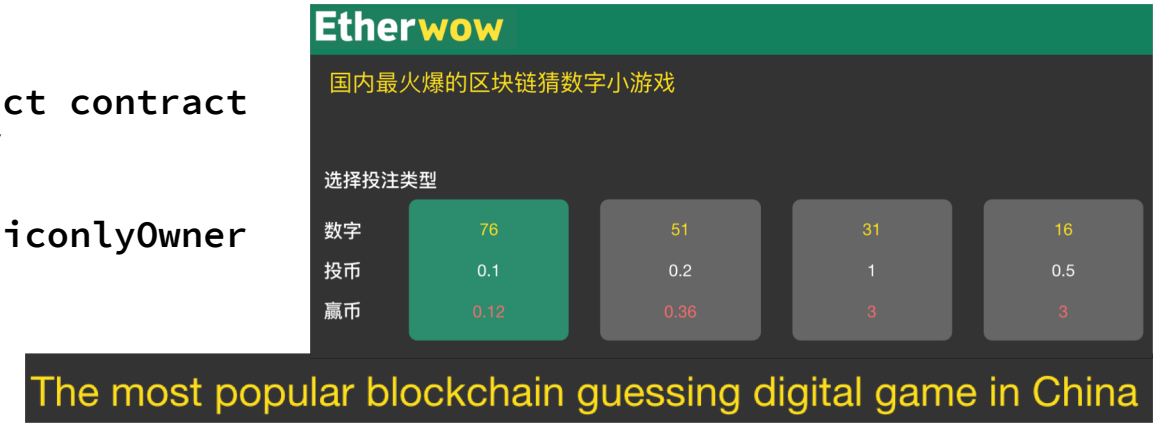
0x4DF6DE08D11f11EBAd5d9E136B768849426fB8a7

Function: ownerChangeOwner(address newOwner)

MethodID: 0x4f44728d

[0]: 000000000000000000000000007d138be0eed529ae42a468472b2beb0314af5e28

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



.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