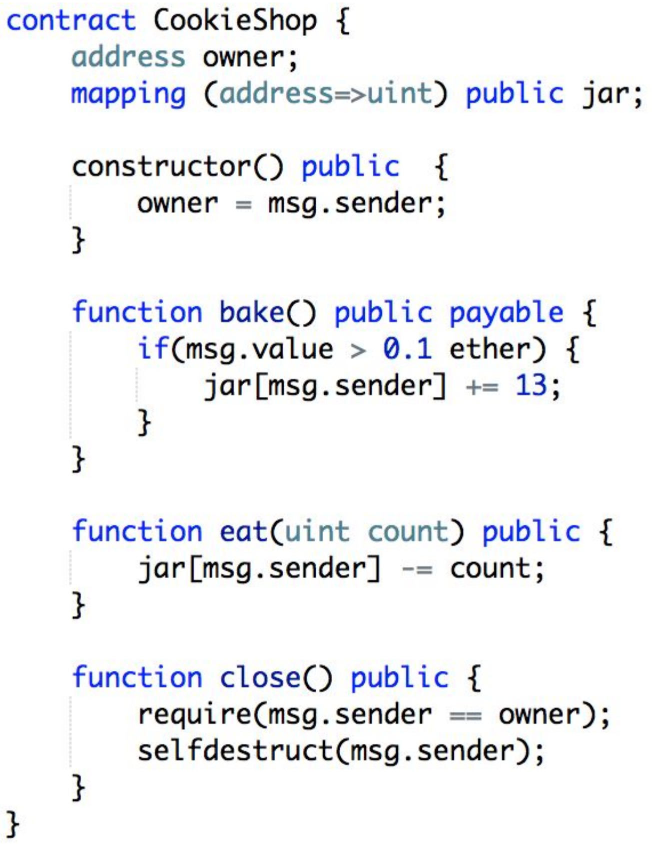
Blockchain Autopsies: Analyzing selfdestructs

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() → □

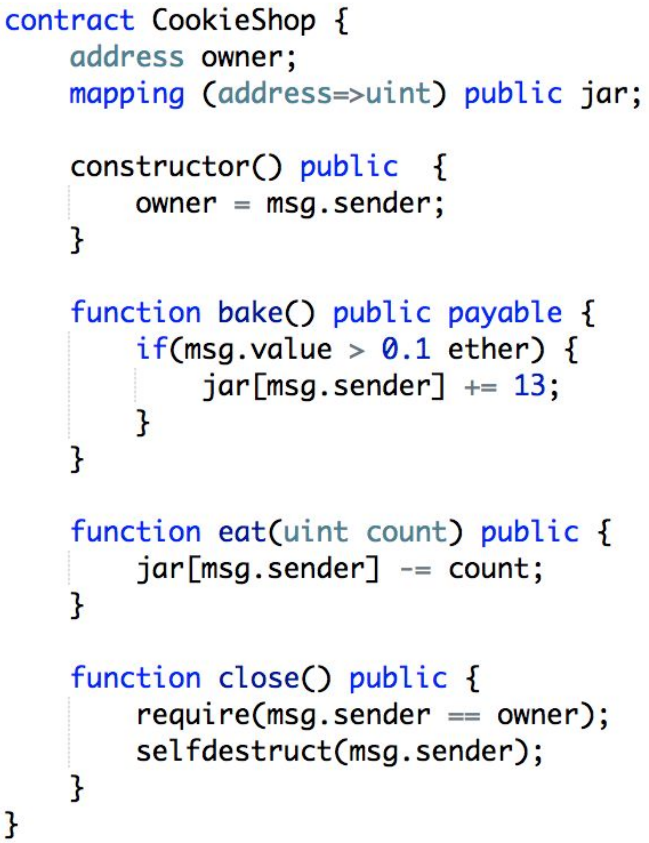
□♂ → bake() → □

□ 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:[]

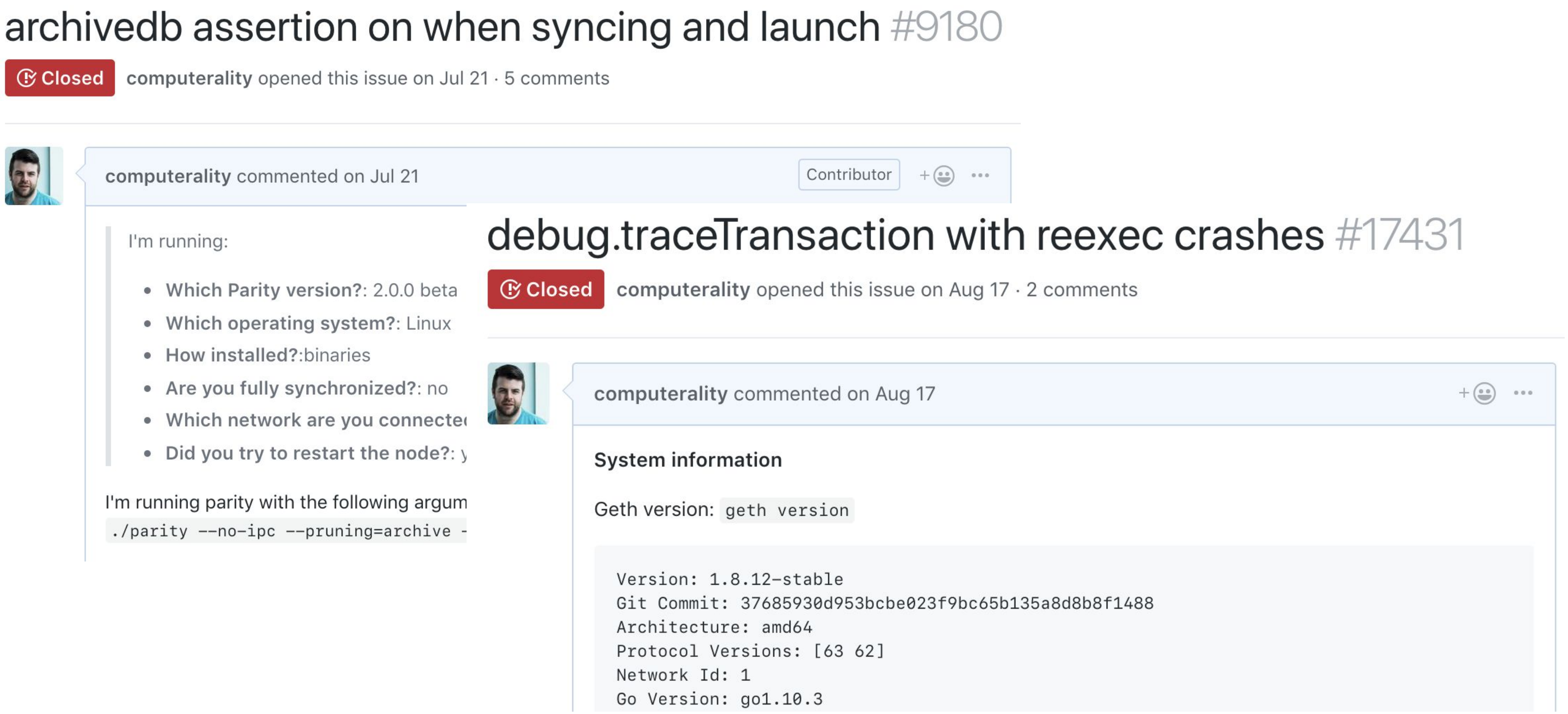
jar[]

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 **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`

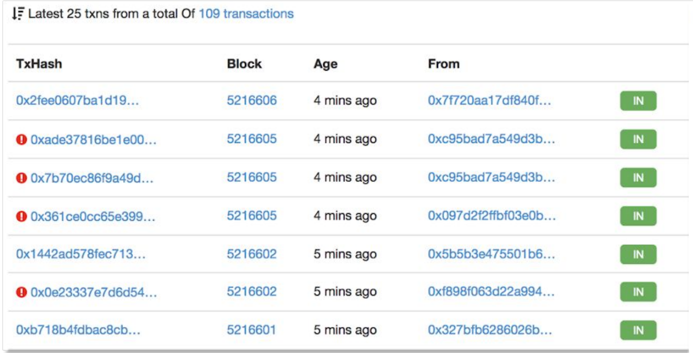
```
Version: 1.8.12-stable
Git Commit: 37685930d953bcbe023f9bc65b135a8d8b8f1488
Architecture: amd64
Protocol Versions: [63 62]
Network Id: 1
Go Version: go1.10.3
```

Hybrid Approach

Full Node + Etherscan API

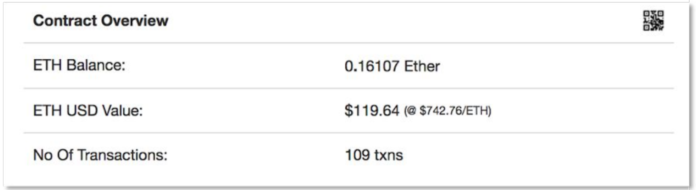
https://etherscan.io/apis

- txlist
- txlistinternal



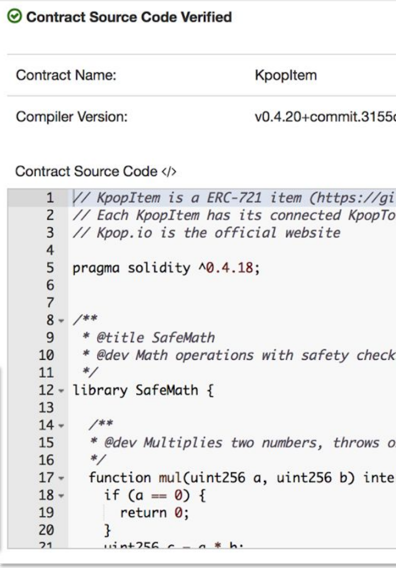
↓≡ Latest 25 txns from a total Of 109 transactions

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



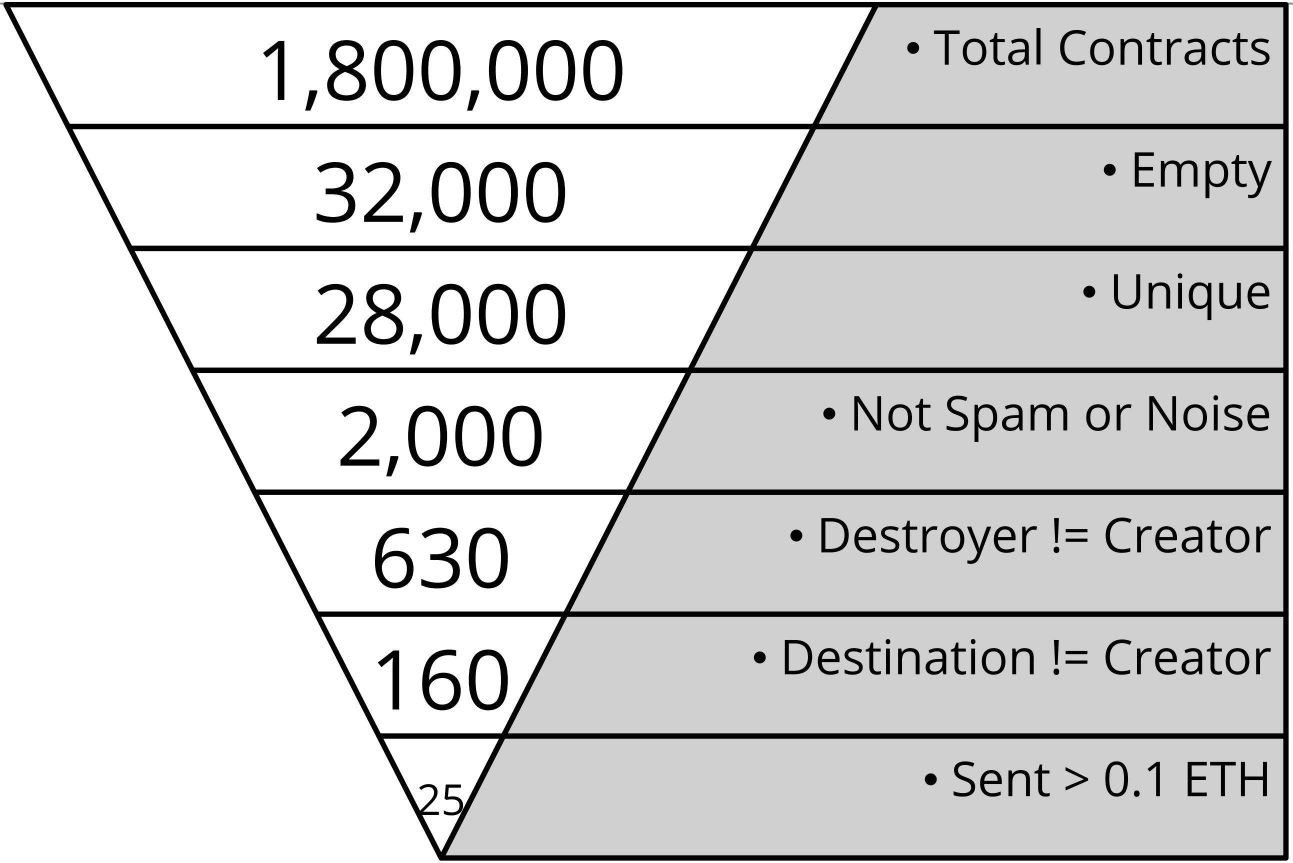
✓ **Contract Source Code Verified**

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

Contract Source Code </>

```
// KpopItem is a ERC-721 item (https://gi
// Each KpopItem has its connected KpopTo
// Kpop.io is the official website

pragma solidity ^0.4.18;


/**
 * @title SafeMath
 * @dev Math operations with safety check
 */
library SafeMath {

  /**
  * @dev Multiplies two numbers, throws o
  */
  function mul(uint256 a, uint256 b) inte
    if (a == 0) {
      return 0;
    }
    uint256 c = a * b;
```

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



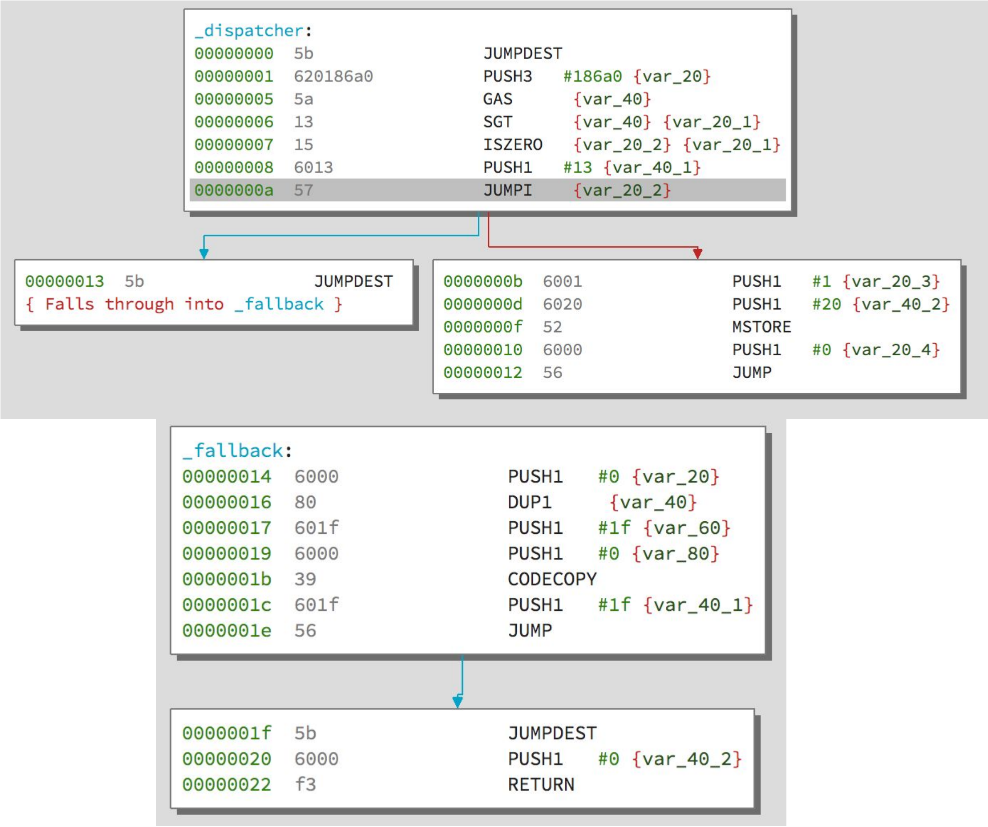
1,800,000	• Total Contracts
32,000	• Empty
28,000	• Unique
2,000	• Not Spam or Noise
630	• Destroyer != Creator
160	• Destination != Creator
25	• Sent > 0.1 ETH

Top Duplicates

Count: 10,072

Code:

```
0x5b620186a05a1315
6013576001602052600
0565b600080601f60
0039601f565b6000f3
```



```
_dispatcher:
00000000  5b             JUMPDEST
00000001  620186a0       PUSH3    #186a0 {var_20}
00000005  5a             GAS       {var_40}
00000006  13             SGT       {var_40} {var_20_1}
00000007  15             ISZERO    {var_20_2} {var_20_1}
00000008  6013           PUSH1    #13 {var_40_1}
0000000a  57             JUMPI     {var_20_2}
```

```
00000013  5b             JUMPDEST
{ Falls through into _fallback }
```

```
0000000b  6001           PUSH1    #1 {var_20_3}
0000000d  6020           PUSH1    #20 {var_40_2}
0000000f  52             MSTORE
00000010  6000           PUSH1    #0 {var_20_4}
00000012  56             JUMP
```

```
_fallback:
00000014  6000           PUSH1    #0 {var_20}
00000016  80             DUP1      {var_40}
00000017  601f           PUSH1    #1f {var_60}
00000019  6000           PUSH1    #0 {var_80}
0000001b  39             CODECOPY
0000001c  601f           PUSH1    #1f {var_40_1}
0000001e  56             JUMP
```

```
0000001f  5b             JUMPDEST
00000020  6000           PUSH1    #0 {var_40_2}
00000022  f3             RETURN
```

Top Duplicates (2)

Count: 9,512

Code:

```
0x
```

Total: 6203 ETH

Top Duplicates (3)

Count: 1,963

Code:

```
0x00000000000000000000000000000000000000000000000
000000000000000000…00000000000000000000
```

6000 NULs (STOP)

*EIP-170 sets max size to 0x6000

Noise / Spam

0x7F62E6C7Ec6700187aB99f71997912A9CDF184D1

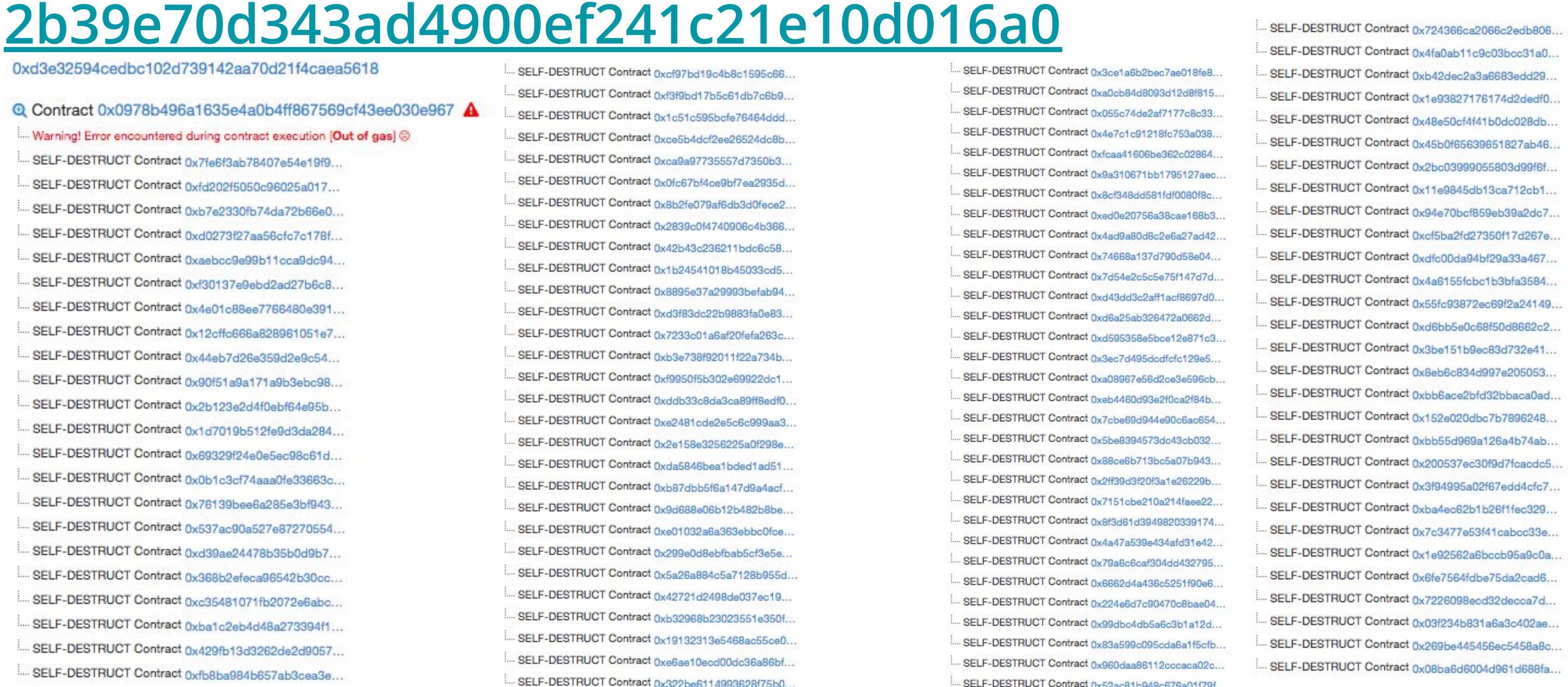
```
PUSH20 0xff5932556071d5ac315d240b92b97a3b4f7daf3d
SELFDESTRUCT
```

0, 1 or 2 Wei transferred

~3,000 instances of this

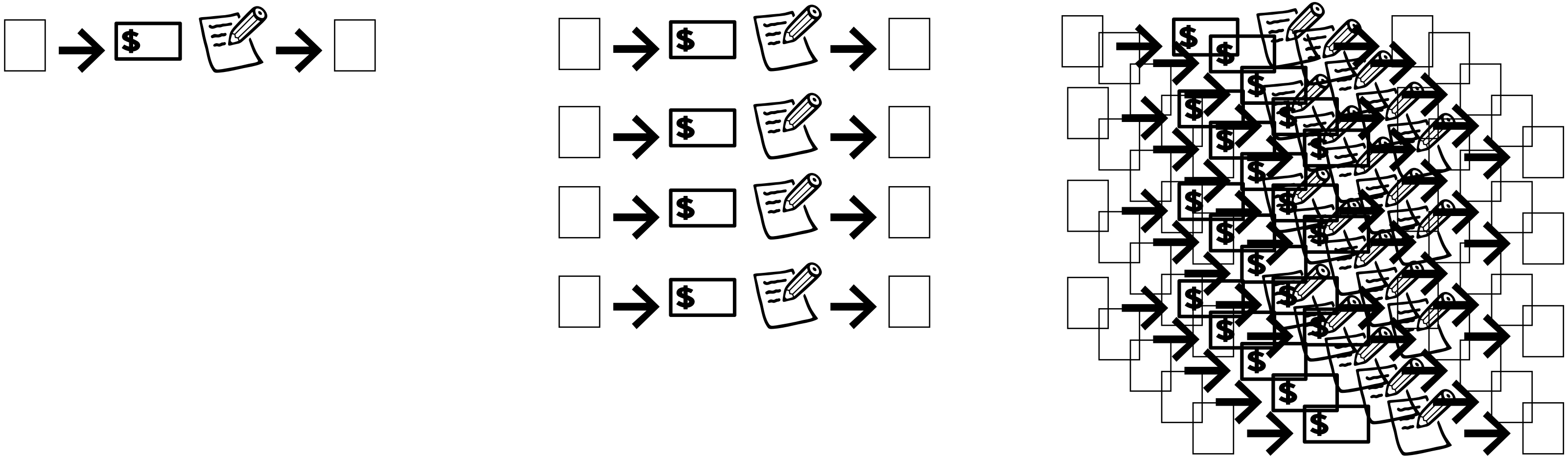
Massive chained selfdestruct

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



```
0xd3e32594cedbc102d739142aa70d21f4caea5618

Contract 0x0978b496a1635e4a0b4ff867569cf43ee030e967
  Warning! Error encountered during contract execution [Out of gas]
  SELF-DESTRUCT Contract 0x7fe6f3ab78407e54e19f9...
  SELF-DESTRUCT Contract 0xfd202f5050c96025a017...
  SELF-DESTRUCT Contract 0xb7e2330fb74da72b66e0...
  SELF-DESTRUCT Contract 0xd0273f27aa56cfc7c178f...
  SELF-DESTRUCT Contract 0xaebcc9e99b11cca9dc94...
  SELF-DESTRUCT Contract 0xf30137e9ebd2ad27b6c8...
  SELF-DESTRUCT Contract 0x4e01c88ee7766480e391...
  SELF-DESTRUCT Contract 0x12cffc666a828961051e7...
  SELF-DESTRUCT Contract 0x44eb7d26e359d2e9c54...
  SELF-DESTRUCT Contract 0x90f51a9a171a9b3ebc98...
  SELF-DESTRUCT Contract 0x2b123e2d4f0ebf64e95b...
  SELF-DESTRUCT Contract 0x1d7019b512fe9d3da284...
  SELF-DESTRUCT Contract 0x69329f24e0e5ec98c61d...
  SELF-DESTRUCT Contract 0x0b1c3cf74aaa0fe33663c...
  SELF-DESTRUCT Contract 0x76139bee6a285e3bf943...
  SELF-DESTRUCT Contract 0x537ac90a527e87270554...
  SELF-DESTRUCT Contract 0xd39ae24478b35b0d9b7...
  SELF-DESTRUCT Contract 0x368b2efeca96542b30cc...
  SELF-DESTRUCT Contract 0xc35481071fb2072e6abc...
  SELF-DESTRUCT Contract 0xba1c2eb4d48a273394f1...
  SELF-DESTRUCT Contract 0x429fb13d3262de2d9057...
  SELF-DESTRUCT Contract 0xfb8ba984b657ab3cea3e...

  SELF-DESTRUCT Contract 0xcf97bd19c4b8c1595c66...
  SELF-DESTRUCT Contract 0xf3f9bd17b5c61db7c6b9...
  SELF-DESTRUCT Contract 0x1c51c595bcfe76464ddd...
  SELF-DESTRUCT Contract 0xce5b4dcf2ee26524dc8b...
  SELF-DESTRUCT Contract 0xca9a97735557d7350b3...
  SELF-DESTRUCT Contract 0x0fc67bf4ce9bf7ea2935d...
  SELF-DESTRUCT Contract 0x8b2fe079af6db3d0fece2...
  SELF-DESTRUCT Contract 0x2839c0f4740906c4b366...
  SELF-DESTRUCT Contract 0x42b43c236211bdc6c58...
  SELF-DESTRUCT Contract 0x1b24541018b45033cd5...
  SELF-DESTRUCT Contract 0x8895e37a29993befab94...
  SELF-DESTRUCT Contract 0xd3f83dc22b9883fa0e83...
  SELF-DESTRUCT Contract 0x7233c01a6af20fefa263c...
  SELF-DESTRUCT Contract 0xb3e738f92011f22a734b...
  SELF-DESTRUCT Contract 0xf9950f5b302e69922dc1...
  SELF-DESTRUCT Contract 0xddb33c8da3ca89ff8edf0...
  SELF-DESTRUCT Contract 0xe2481cde2e5c6c999aa3...
  SELF-DESTRUCT Contract 0x2e158e3256225a0f298e...
  SELF-DESTRUCT Contract 0xda5846bea1bded1ad51...
  SELF-DESTRUCT Contract 0xb87dbb5f6a147d9a4acf...
  SELF-DESTRUCT Contract 0x9d688e06b12b482b8be...
  SELF-DESTRUCT Contract 0xe01032a6a363ebbc0fce...
  SELF-DESTRUCT Contract 0x299e0d8ebfbab5cf3e5e...
  SELF-DESTRUCT Contract 0x5a26a884c5a7128b955d...
  SELF-DESTRUCT Contract 0x42721d2498de037ec19...
  SELF-DESTRUCT Contract 0xb32968b23023551e350f...
  SELF-DESTRUCT Contract 0x19132313e5468ac55ce0...
  SELF-DESTRUCT Contract 0xe6ae10ecd00dc36a86bf...
  SELF-DESTRUCT Contract 0x322be6114993628f75b0...

  SELF-DESTRUCT Contract 0x3ce1a6b2bec7ae018fe8...
  SELF-DESTRUCT Contract 0xa0cb84d8093d12d8f815...
  SELF-DESTRUCT Contract 0x055c74de2af7177c8c33...
  SELF-DESTRUCT Contract 0x4e7c1c91218fc753a038...
  SELF-DESTRUCT Contract 0xfcaa41606be362c02864...
  SELF-DESTRUCT Contract 0x9a310671bb1795127aec...
  SELF-DESTRUCT Contract 0x8cf348dd581fdf0080f8c...
  SELF-DESTRUCT Contract 0xed0e20756a38cae168b3...
  SELF-DESTRUCT Contract 0x4ad9a80d8c2e6a27ad42...
  SELF-DESTRUCT Contract 0x74668a137d790d58e04...
  SELF-DESTRUCT Contract 0x7d54e2c5c5e75f147d7d...
  SELF-DESTRUCT Contract 0xd43dd3c2aff1acf8697d0...
  SELF-DESTRUCT Contract 0xd6a25ab326472a0662d...
  SELF-DESTRUCT Contract 0xd595358e5bce12e871c3...
  SELF-DESTRUCT Contract 0x3ec7d495dcdfcfc129e5...
  SELF-DESTRUCT Contract 0xa08967e56d2ce3e596cb...
  SELF-DESTRUCT Contract 0xeb4460d93e2f0ca2f84b...
  SELF-DESTRUCT Contract 0x7cbe69d944e90c6ac654...
  SELF-DESTRUCT Contract 0x5be8394573dc43cb032...
  SELF-DESTRUCT Contract 0x88ce6b713bc5a07b943...
  SELF-DESTRUCT Contract 0x2ff39d3f20f3a1e26229b...
  SELF-DESTRUCT Contract 0x7151cbe210a214faee22...
  SELF-DESTRUCT Contract 0x8f3d61d3949820339174...
  SELF-DESTRUCT Contract 0x4a47a539e434afd31e42...
  SELF-DESTRUCT Contract 0x79a6c6caf304dd432795...
  SELF-DESTRUCT Contract 0x6662d4a436c5251f90e6...
  SELF-DESTRUCT Contract 0x224e6d7c90470c8bae04...
  SELF-DESTRUCT Contract 0x99dbc4db5a6c3b1a12d...
  SELF-DESTRUCT Contract 0x83a599c095cda6a1f5cfb...
  SELF-DESTRUCT Contract 0x960daa86112cccaca02c...
  SELF-DESTRUCT Contract 0x52ac81b948c676a01f79f

  SELF-DESTRUCT Contract 0x724366ca2066c2edb806...
  SELF-DESTRUCT Contract 0x4fa0ab11c9c03bcc31a0...
  SELF-DESTRUCT Contract 0xb42dec2a3a6683edd29...
  SELF-DESTRUCT Contract 0x1e93827176174d2dedf0...
  SELF-DESTRUCT Contract 0x48e50cf4f41b0dc028db...
  SELF-DESTRUCT Contract 0x45b0f65639651827ab46...
  SELF-DESTRUCT Contract 0x2bc03999055803d99f6f...
  SELF-DESTRUCT Contract 0x11e9845db13ca712cb1...
  SELF-DESTRUCT Contract 0x94e70bcf859eb39a2dc7...
  SELF-DESTRUCT Contract 0xcf5ba2fd27350f17d267e...
  SELF-DESTRUCT Contract 0xdfc00da94bf29a33a467...
  SELF-DESTRUCT Contract 0x4a6155fcbc1b3bfa3584...
  SELF-DESTRUCT Contract 0x55fc93872ec69f2a24149...
  SELF-DESTRUCT Contract 0xd6bb5e0c68f50d8662c2...
  SELF-DESTRUCT Contract 0x3be151b9ec83d732e41...
  SELF-DESTRUCT Contract 0x8eb6c834d997e205053...
  SELF-DESTRUCT Contract 0xbb6ace2bfd32bbaca0ad...
  SELF-DESTRUCT Contract 0x152e020dbc7b7896248...
  SELF-DESTRUCT Contract 0xbb55d969a126a4b74ab...
  SELF-DESTRUCT Contract 0x200537ec30f9d7fcacdc5...
  SELF-DESTRUCT Contract 0x3f94995a02f67edd4cfc7...
  SELF-DESTRUCT Contract 0xba4ec62b1b26f1fec329...
  SELF-DESTRUCT Contract 0x7c3477e53f41cabcc33e...
  SELF-DESTRUCT Contract 0x1e92562a6bccb95a9c0a...
  SELF-DESTRUCT Contract 0x6fe7564fdbe75da2cad6...
  SELF-DESTRUCT Contract 0x7226098ecd32decca7d...
  SELF-DESTRUCT Contract 0x03f234b831a6a3c402ae...
  SELF-DESTRUCT Contract 0x269be445456ec5458a8c...
  SELF-DESTRUCT Contract 0x08ba6d6004d961d688fa...
```

Massive selfdestruct



2000

2000 □ → 📝 → □ → 💥💵 → □

630 □ → 📝 → □ → 💥💵 → □

160 □□♂ → 📝 → □ → 💥💵 → □□♂

16 □□♂ → 📝 → □ → 💥💰💰(1ETH) → □□♂

50ETH to 0x0

0xf73d247ffDBD5A9964d1a1444c86343650b67ed4

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

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

[0]:
0000000000000000000000000000000000000000000000000
000000000000000
```

300ETH selfdestruct

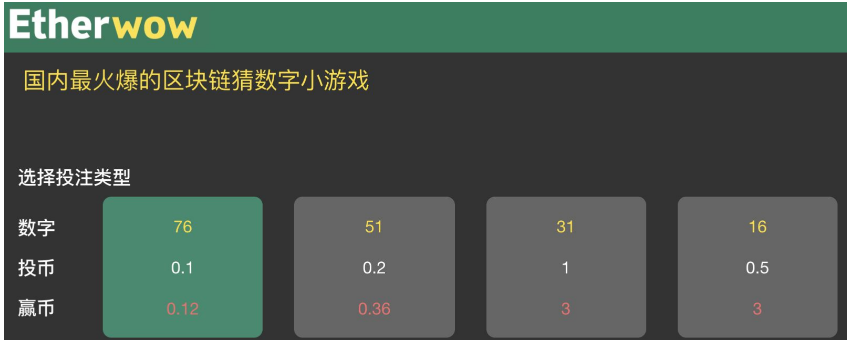
```
Account:0x96f65700904cB464F3D153a2744B84FCa27ABF9C

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]:  0000000000000000000000007d138be0eed529ae42a468472b2beb0314af5e28

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
投币	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

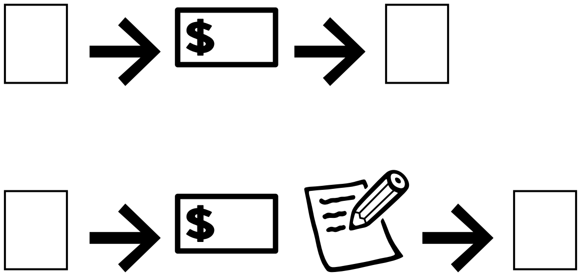
Jay Little, Principal Security Engineer
jay@trailofbits.com
@computerality

@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