长亭科技
CHAITIN

协议设计缺陷

from a code auditing perspective

目录 Table Of Content

长亭科技
CHAITIN

- 通讯协议要素分析
- 常见协议漏洞
- 从协议要素角度看区块链漏洞
- 智能合约审计从”新”出发

通讯协议要素

- 1 数据格式&地址格式
- 2 完整校验&纠错
- 3 收信应答
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制
- 7 分片控制
- 8 地址映射&路由

https://en.wikipedia.org/wiki/Communication_protocol

Comms. protocol essentials

长亭科技 CHAITIN

- 1 数据格式&地址格式 Data/Address format
- 2 完整校验&纠错 Detection of TX errors
- 3 收信应答 Acknowledgements
- 4 超时&重试 Timeouts & retries
- 5 数据流方向 Direction of information flow
- 6 流程顺序控制 Flow control
- 7 分片控制 Sequence control
- 8 地址映射&路由 Address mapping & Routing

通讯协议要素

长亭科技
CHAITIN

- 1 数据格式&地址格式
- 2 完整校验&纠错
- 3 收信应答
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制
- 7 分片控制
- 8 地址映射&路由

MySQL over TCP

流程顺序控制 Flow control

服务器你好

客户端你好这是我的版本号及支持的认证方式等信息

请按照这组用户名密码让我登录

Response OK 好嘞 ~

select @@version

5.6.28

LOAD DATA LOCAL INFILE ‘/etc/passwd’ INTO TABLE test FIELDS TERMINATED BY ‘\n’

行啊，test我给你准备好了，把/etc/passwd发来吧。

好嘞，文件内容是
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
…

MySQL over TCP

服务器你好

客户端你好这是我的版本号及支持的认证方式等信息

请按照这组用户名密码让我登录

Response OK 好嘞 ~

select @@version

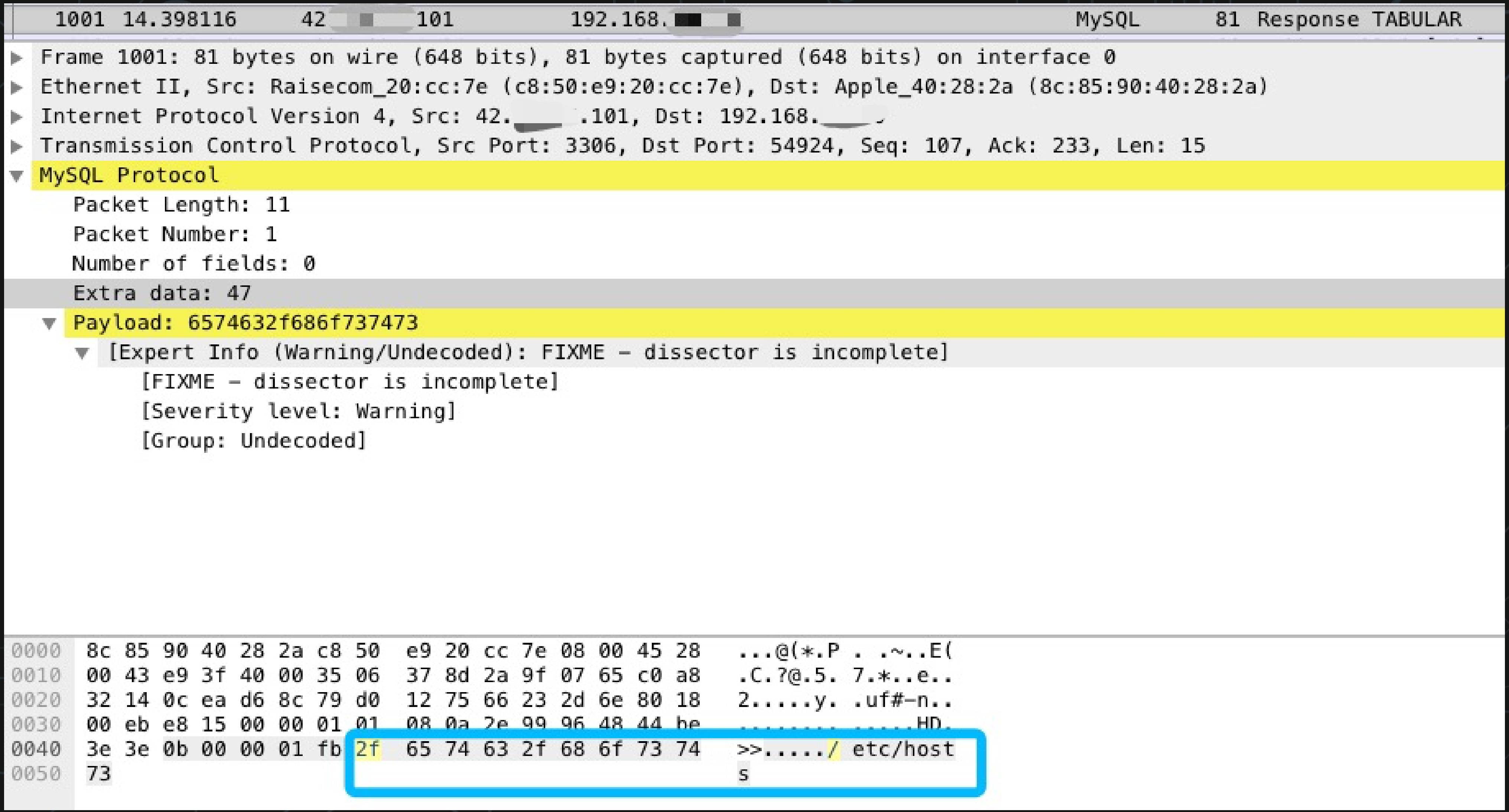
5.6.28

LOAD DATA LOCAL INFILE '/etc/passwd' INTO TABLE test FIELDS TERMINATED BY '\n'

行啊，test我给你准备好了，把/etc/passwd发来吧。

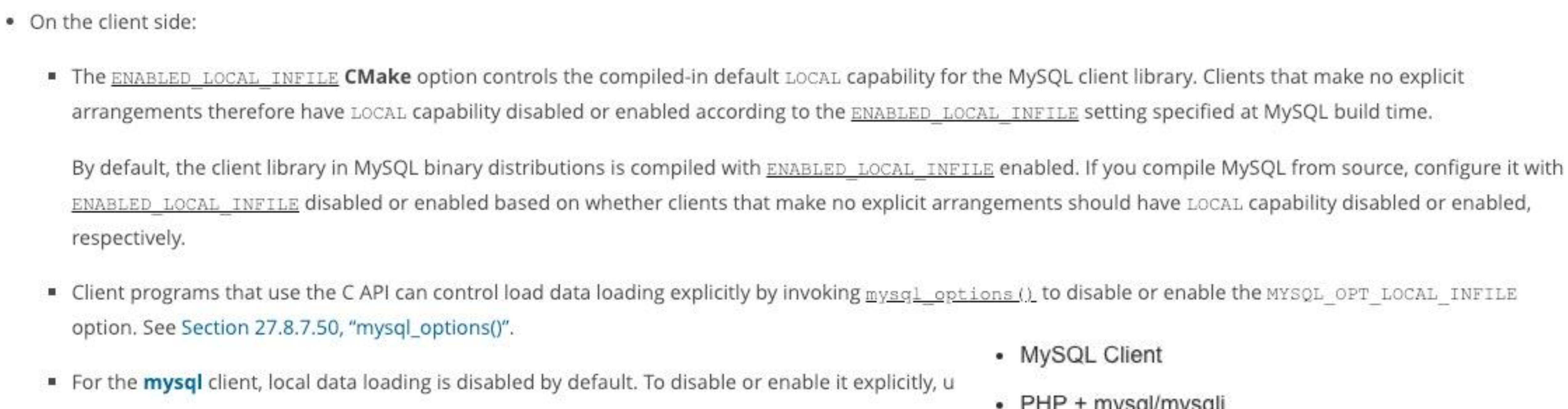
好嘞，文件内容是
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
...

管中窥豹 Into the traffic...



```
   1001  14.398116     42.[redacted]101         192.168.[redacted]                        MySQL      81  Response TABULAR
▶ Frame 1001: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶ Ethernet II, Src: Raisecom_20:cc:7e (c8:50:e9:20:cc:7e), Dst: Apple_40:28:2a (8c:85:90:40:28:2a)
▶ Internet Protocol Version 4, Src: 42.[redacted].101, Dst: 192.168.[redacted]
▶ Transmission Control Protocol, Src Port: 3306, Dst Port: 54924, Seq: 107, Ack: 233, Len: 15
▼ MySQL Protocol
    Packet Length: 11
    Packet Number: 1
    Number of fields: 0
    Extra data: 47
  ▼ Payload: 6574632f686f737473
    ▼ [Expert Info (Warning/Undecoded): FIXME - dissector is incomplete]
        [FIXME - dissector is incomplete]
        [Severity level: Warning]
        [Group: Undecoded]

0000  8c 85 90 40 28 2a c8 50  e9 20 cc 7e 08 00 45 28   ...@(*.P . .~..E(
0010  00 43 e9 3f 40 00 35 06  37 8d 2a 9f 07 65 c0 a8   .C.?@.5. 7.*..e..
0020  32 14 0c ea d6 8c 79 d0  12 75 66 23 2d 6e 80 18   2.....y. .uf#-n..
0030  00 eb e8 15 00 00 01 01  08 0a 2e 99 96 48 44 be   ........ ......HD.
0040  3e 3e 0b 00 00 01 fb 2f  65 74 63 2f 68 6f 73 74   >>...../ etc/host
0050  73                                                 s
```

Patch the client 发行方的建议



- On the client side:
  - The ENABLED_LOCAL_INFILE **CMake** option controls the compiled-in default LOCAL capability for the MySQL client library. Clients that make no explicit arrangements therefore have LOCAL capability disabled or enabled according to the ENABLED_LOCAL_INFILE setting specified at MySQL build time.

    By default, the client library in MySQL binary distributions is compiled with ENABLED_LOCAL_INFILE enabled. If you compile MySQL from source, configure it with ENABLED_LOCAL_INFILE disabled or enabled based on whether clients that make no explicit arrangements should have LOCAL capability disabled or enabled, respectively.
  - Client programs that use the C API can control load data loading explicitly by invoking mysql_options() to disable or enable the MYSQL_OPT_LOCAL_INFILE option. See Section 27.8.7.50, “mysql_options()”.
  - For the **mysql** client, local data loading is disabled by default. To disable or enable it explicitly, u

- MySQL Client
- PHP + mysql/mysqli
- PHP + PDO (MYSQL_ATTR_LOCAL_INFILE)
- Python + MySQLdb
- Python3 + mysqlclient
- Java + JDBC Driver
- ...

A solid advice, or is it?

https://dev.mysql.com/doc/refman/8.0/en/load-data-local.html

MySQL over TCP

长亭科技 CHAITIN

服务器你好

客户端你好这是我的版本号及支持的认证方式等信息

请按照这组用户名密码让我登录

Response OK 好嘞 ~

LOAD DATA LOCAL INFILE ‘/etc/passwd’ INTO TABLE test FIELDS TERMINATED BY ‘\n’

🚫 行啊，test我给你准备好了，把 /etc/passwd发来吧。

行啊，test我给你准备好了，把 内容发来吧。

好嘞，文件内容是
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
…

Server hangs, does it?

长亭科技 CHAITIN

服务器你好

客户端你好这是我的版本号及支持的认证方式等信息

请按照这组用户名密码让我登录

Response OK 好嘞 ~

LOAD DATA LOCAL INFILE ‘/etc/passwd’ INTO TABLE test FIELDS TERMINATED BY ‘\n’

行啊，test我给你准备好了，把 /etc/passwd发来吧。

行啊，test我给你准备好了，把 内容发来吧。

好嘞，文件内容是
nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
root:*:0:0:System Administrator:/var/root:/bin/sh
…

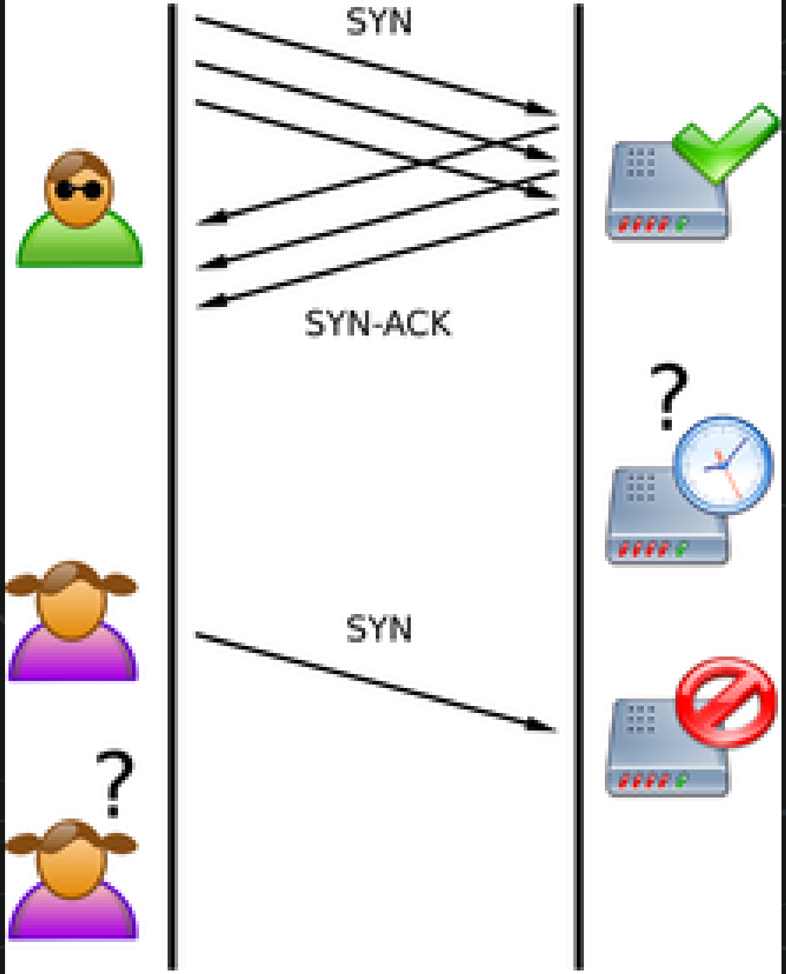
通讯协议要素

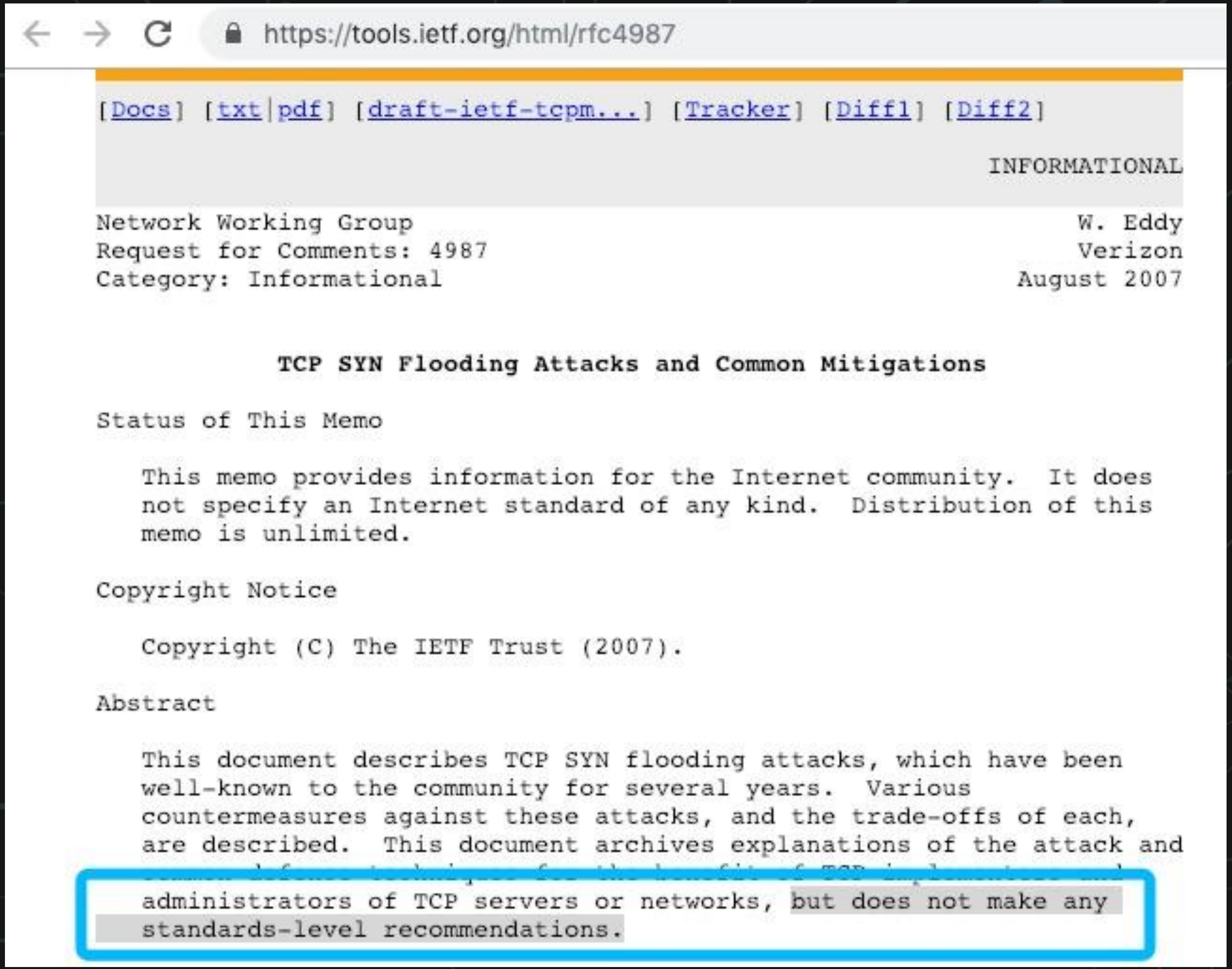
- 1 数据格式&地址格式
- 2 完整校验&纠错
- 3 收信应答
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制
- 7 分片控制
- 8 地址映射&路由

TCP ForTheWin?

你是个成熟的协议了应该学会自己防DOS了。

长亭科技
CHAITIN





```
[Docs] [txt|pdf] [draft-ietf-tcpm...] [Tracker] [Diff1] [Diff2]

                                                        INFORMATIONAL

Network Working Group                                        W. Eddy
Request for Comments: 4987                                   Verizon
Category: Informational                                  August 2007


          TCP SYN Flooding Attacks and Common Mitigations

Status of This Memo

   This memo provides information for the Internet community.  It does
   not specify an Internet standard of any kind.  Distribution of this
   memo is unlimited.

Copyright Notice

   Copyright (C) The IETF Trust (2007).

Abstract

   This document describes TCP SYN flooding attacks, which have been
   well-known to the community for several years.  Various
   countermeasures against these attacks, and the trade-offs of each,
   are described.  This document archives explanations of the attack and
   common defense techniques for the benefit of TCP implementers and
   administrators of TCP servers or networks, but does not make any
   standards-level recommendations.
```

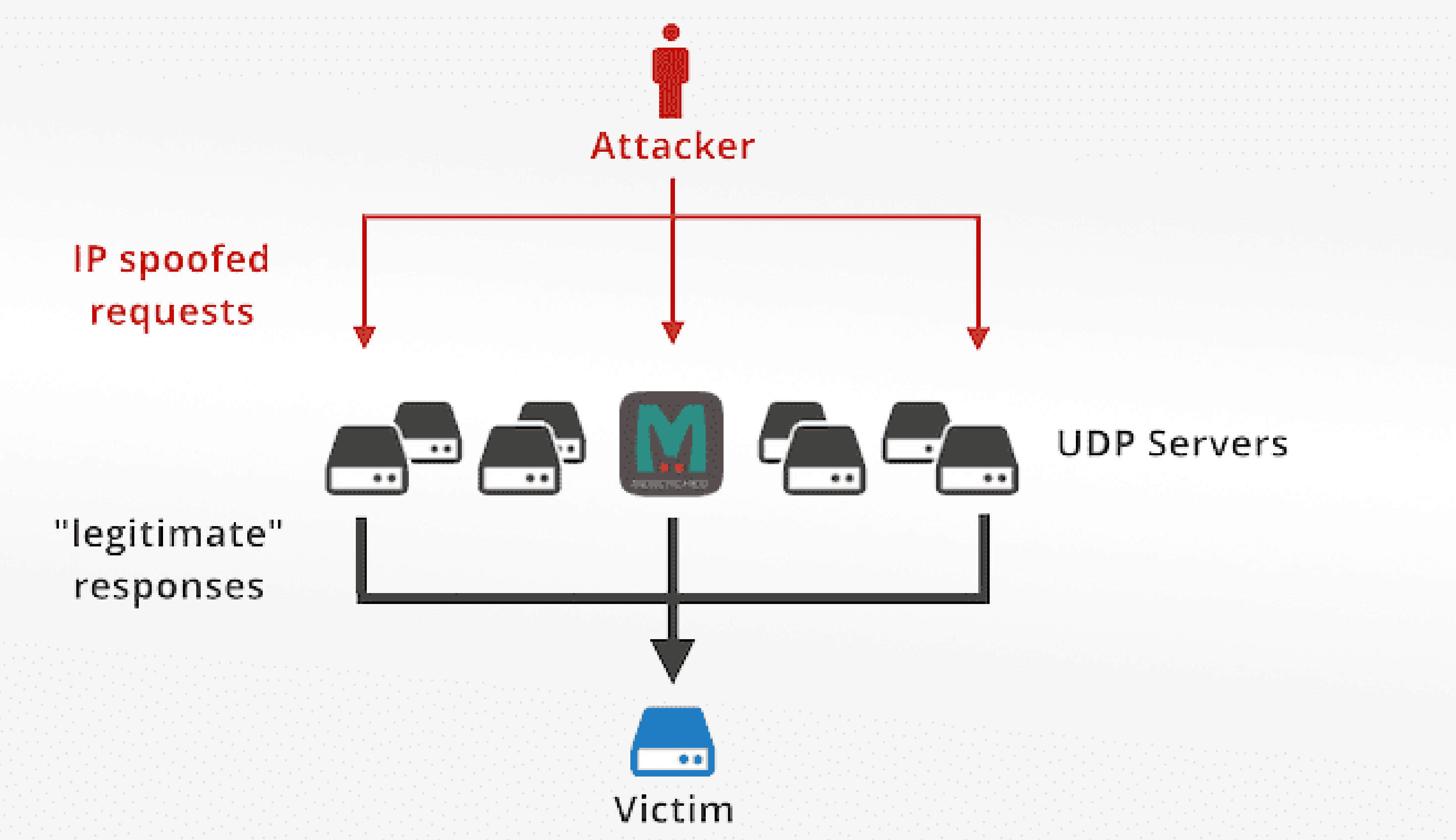
https://en.wikipedia.org/wiki/SYN_flood

通讯协议要素

- 1 数据格式&地址格式
- 2 完整校验&纠错
- 3 收信应答
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制
- 7 分片控制
- 8 地址映射&路由

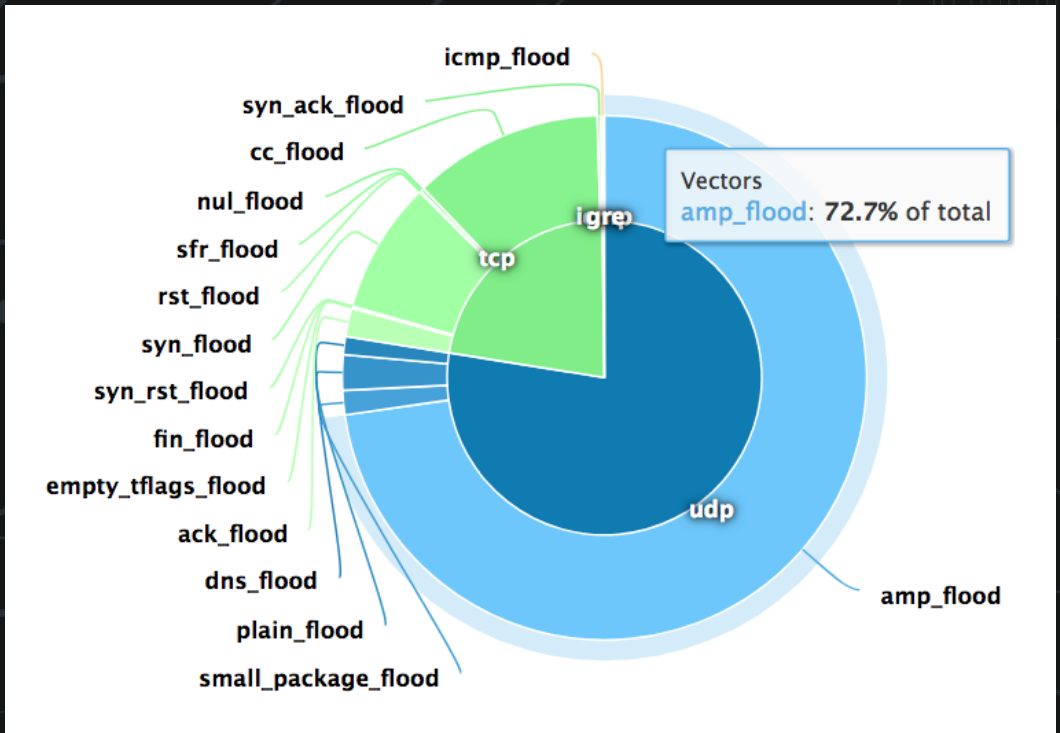
What about UDP

Seems a bit worse



https://www.a10networks.com/resources/articles/how-defend-against-amplified-reflection-ddos-attacks

https://ddosmon.net/insight/?last=7



通讯协议要素

- 1 数据格式&地址格式
- 2 完整校验&纠错
- 3 收信应答
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制
- 7 分片控制
- 8 地址映射&路由

长亭科技
CHAITIN

Heartbleed ?

One important part of the TLS/SSL protocols is what's called a heartbeat.

So if a request said it was 40 KB long but was actually only 20 KB, the receiving computer would set aside 40 KB of memory buffer, then store the 20 KB it actually received, then send back that 20 KB plus whatever happened to be in the next 20 KB of memory. That extra 20 KB of data is information that the attacker has now extracted from the web server.

```
memcpy(bp, pl, payload);
memcpy(bp, pl, sizeof(pl)/sizeof(pl[0]));
```

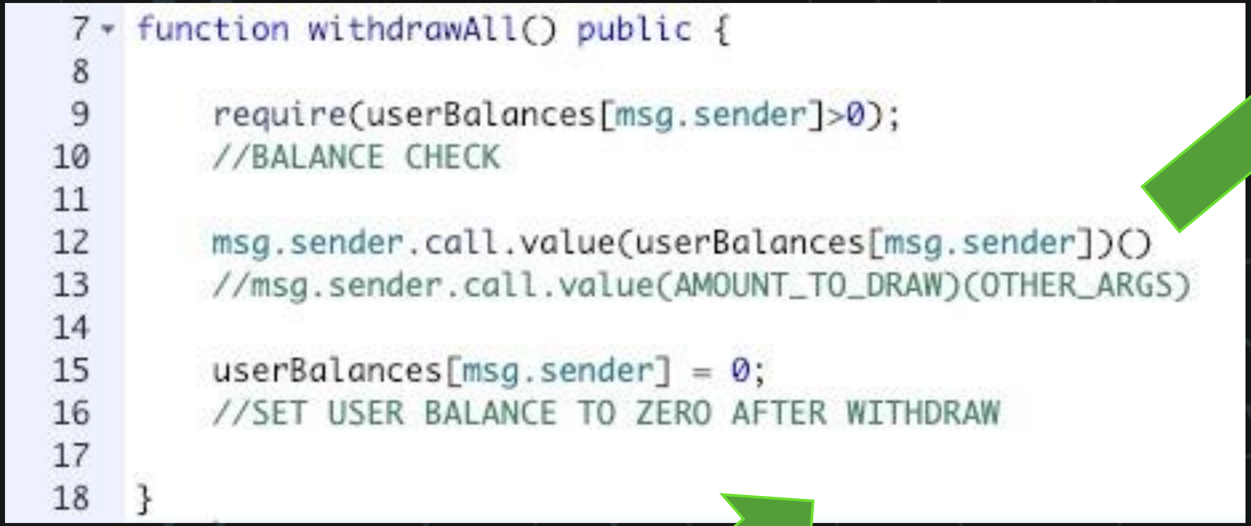
https://www.csoonline.com/article/3223203/vulnerabilities/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html

Comms. in blockchain （ETH）

- 区块链是一个大的分布式系统
- 地址与地址的”交易”即是通信
- 智能合约即是应用层通讯协议
- 智能合约一旦部署无法修改*
- We are talking about writing the MySQL itself rather writing the SQL query.

重入 Reentrancy

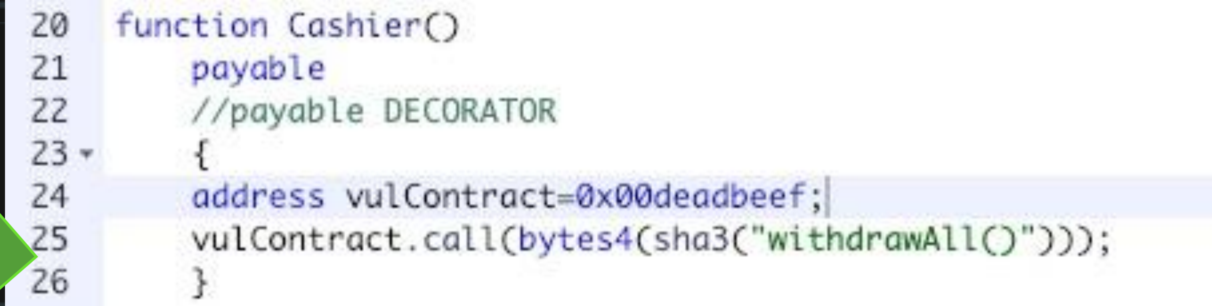
流程顺序控制 Flow control



```
function withdrawAll() public {

    require(userBalances[msg.sender]>0);
    //BALANCE CHECK

    msg.sender.call.value(userBalances[msg.sender])()
    //msg.sender.call.value(AMOUNT_TO_DRAW)(OTHER_ARGS)

    userBalances[msg.sender] = 0;
    //SET USER BALANCE TO ZERO AFTER WITHDRAW

}
```

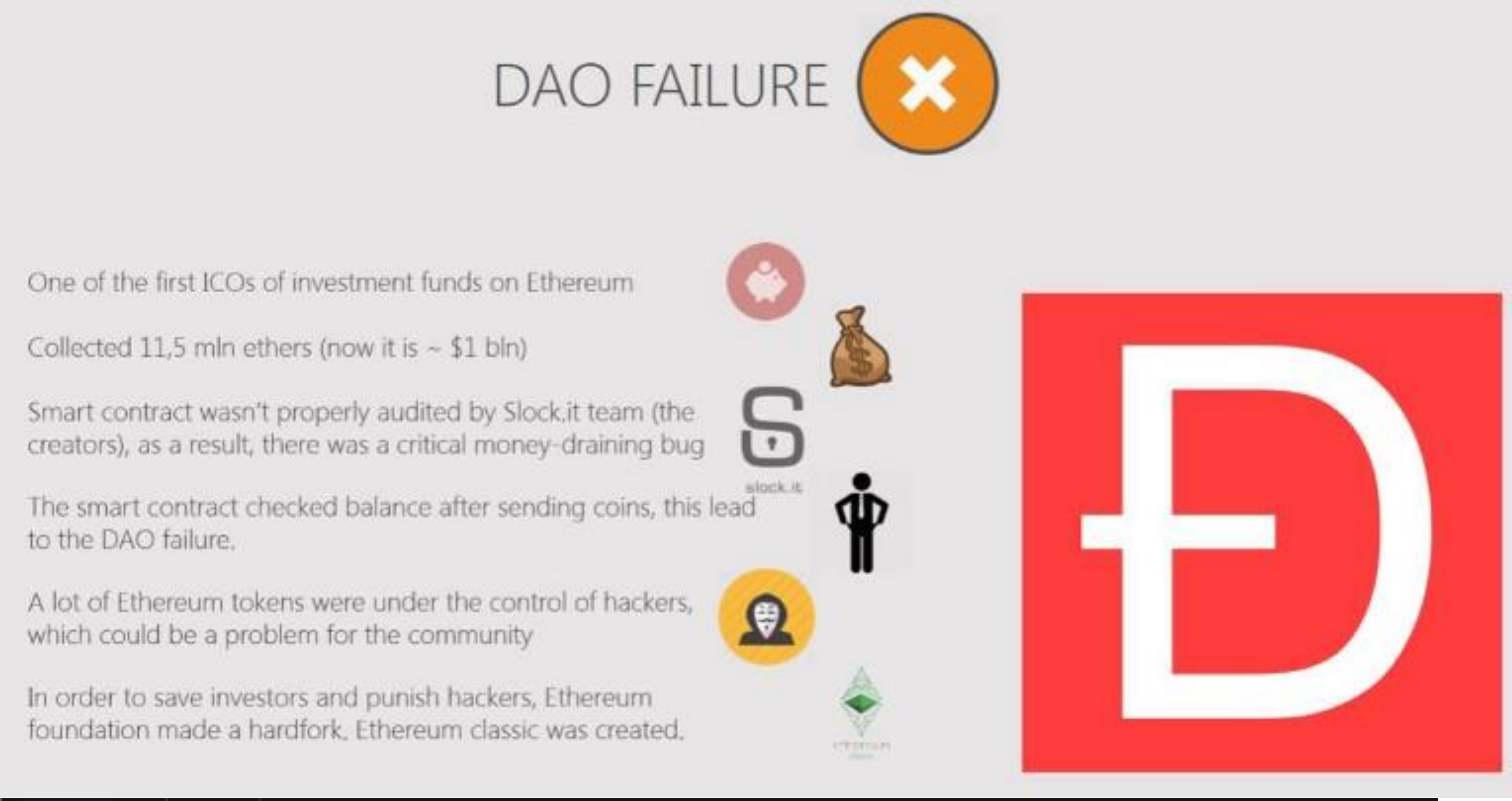
vulContract
存在漏洞的合约

maliciousContract
黑客控制的合约



```
function Cashier()
    payable
    //payable DECORATOR
    {
    address vulContract=0x00deadbeef;
    vulContract.call(bytes4(sha3("withdrawAll()")));
    }
```

Real-world event



DAO FAILURE

One of the first ICOs of investment funds on Ethereum

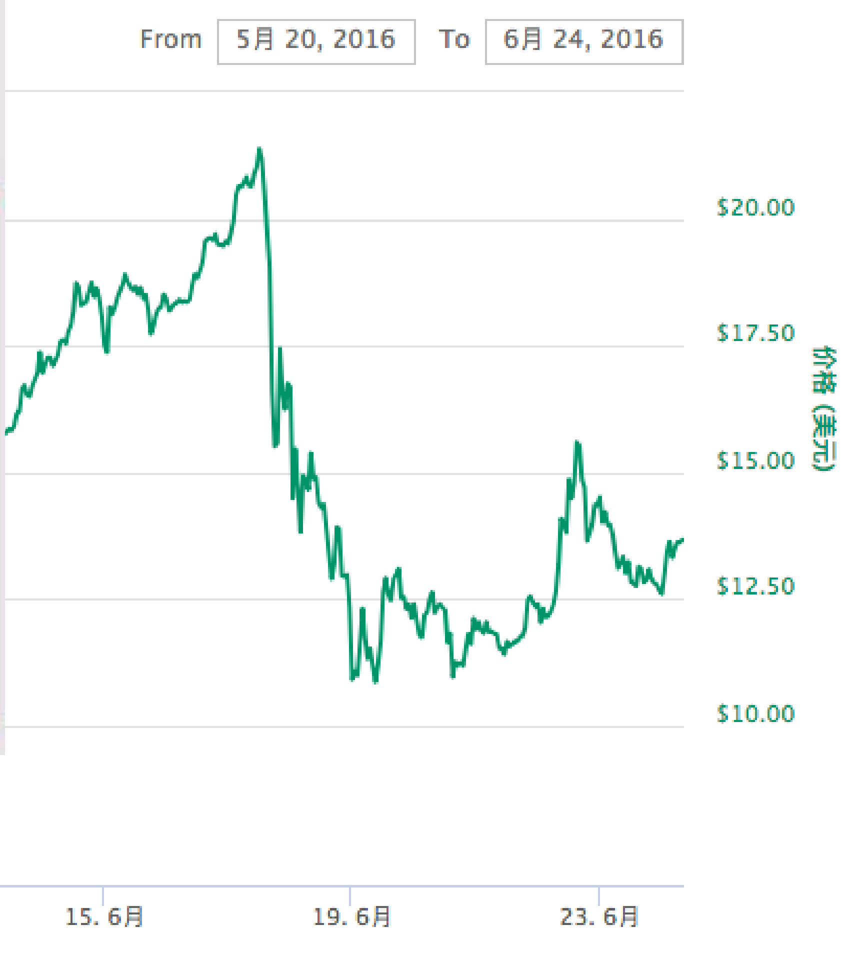
Collected 11,5 mln ethers (now it is ~ $1 bln)

Smart contract wasn't properly audited by Slock.it team (the creators), as a result, there was a critical money-draining bug

The smart contract checked balance after sending coins, this lead to the DAO failure.

A lot of Ethereum tokens were under the control of hackers, which could be a problem for the community

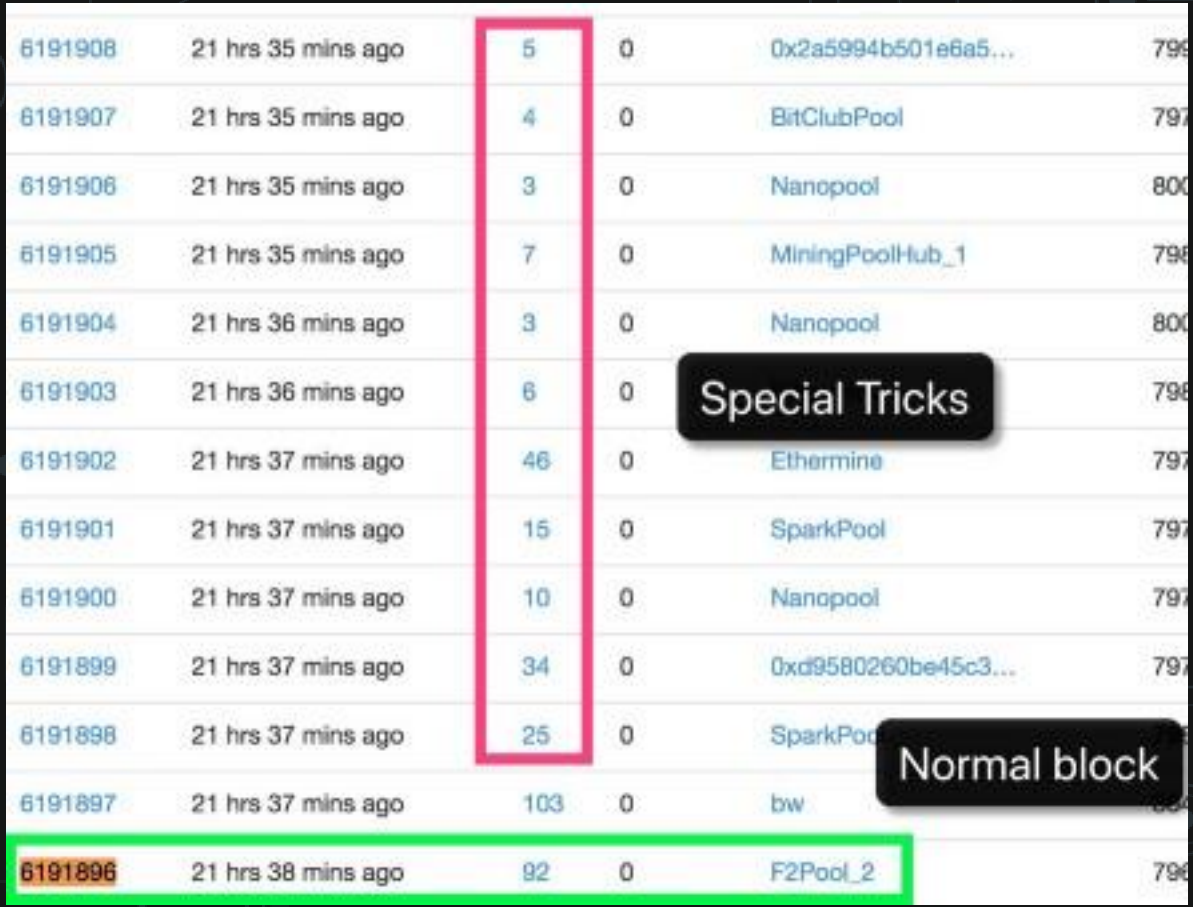
In order to save investors and punish hackers, Ethereum foundation made a hardfork. Ethereum classic was created.



From 5月 20, 2016 To 6月 24, 2016

- Ref. https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

Literally blocks the chain

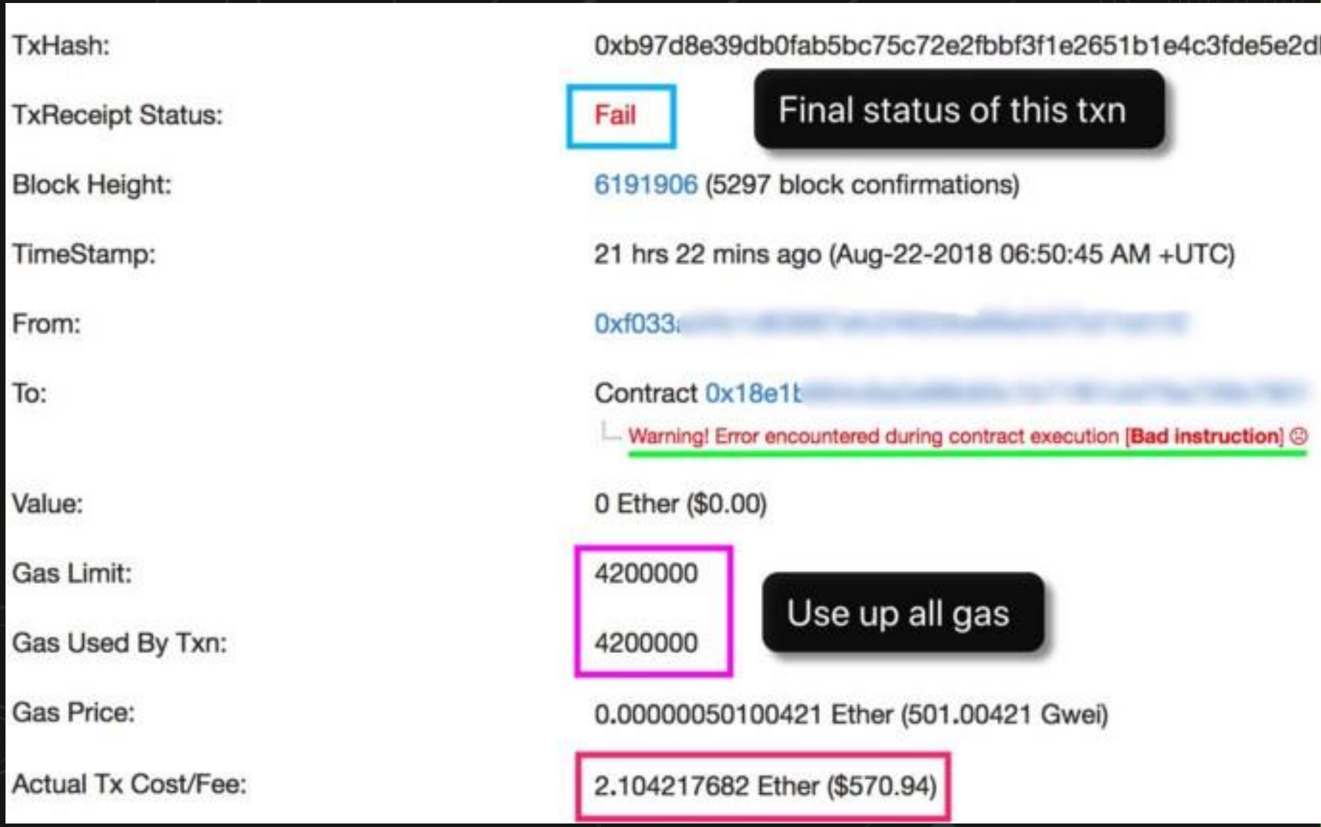


6191908	21 hrs 35 mins ago	5	0	0x2a5994b501e6a5...	799
6191907	21 hrs 35 mins ago	4	0	BitClubPool	797
6191906	21 hrs 35 mins ago	3	0	Nanopool	800
6191905	21 hrs 35 mins ago	7	0	MiningPoolHub_1	798
6191904	21 hrs 36 mins ago	3	0	Nanopool	800
6191903	21 hrs 36 mins ago	6	0	[illegible]	798
6191902	21 hrs 37 mins ago	46	0	Ethermine	797
6191901	21 hrs 37 mins ago	15	0	SparkPool	797
6191900	21 hrs 37 mins ago	10	0	Nanopool	797
6191899	21 hrs 37 mins ago	34	0	0xd9580260be45c3...	797
6191898	21 hrs 37 mins ago	25	0	SparkPo	[illegible]
6191897	21 hrs 37 mins ago	103	0	bw	80
6191896	21 hrs 38 mins ago	92	0	F2Pool_2	796

Special Tricks

Normal block

超时&重试 Timeouts & retries



TxHash:	0xb97d8e39db0fab5bc75c72e2fbbf3f1e2651b1e4c3fde5e2d
TxReceipt Status:	Fail
Block Height:	6191906 (5297 block confirmations)
TimeStamp:	21 hrs 22 mins ago (Aug-22-2018 06:50:45 AM +UTC)
From:	0xf033[redacted]
To:	Contract 0x18e1[redacted] Warning! Error encountered during contract execution [**Bad instruction**] ☹
Value:	0 Ether ($0.00)
Gas Limit:	4200000
Gas Used By Txn:	4200000
Gas Price:	0.00000050100421 Ether (501.00421 Gwei)
Actual Tx Cost/Fee:	2.104217682 Ether ($570.94)

Final status of this txn

Use up all gas

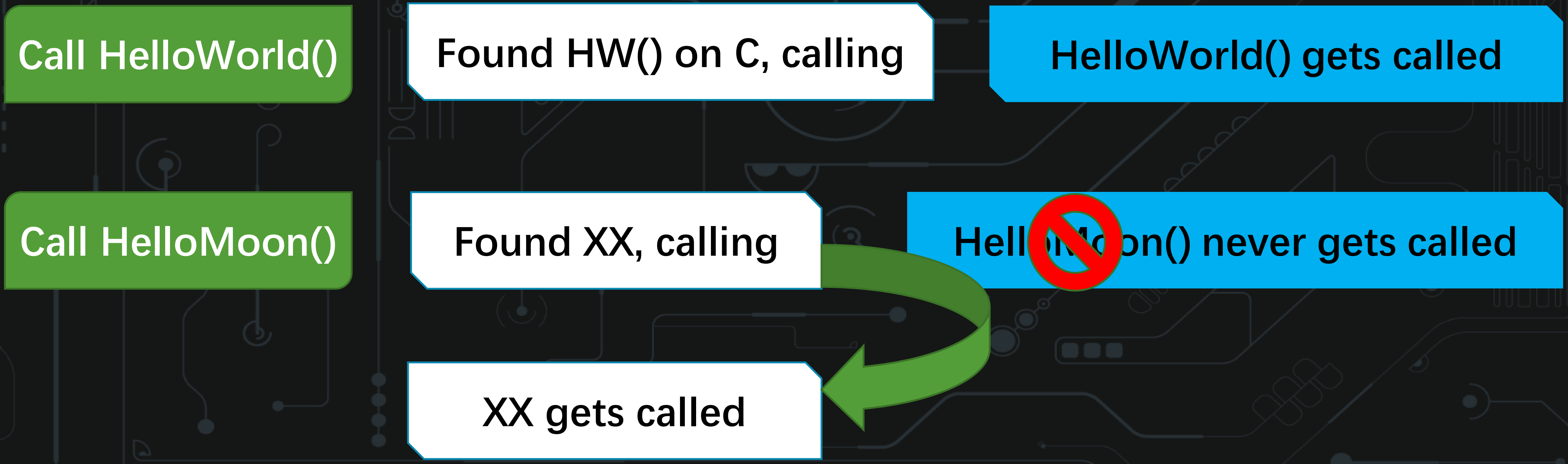
Fomo3D 区块链抽奖拍卖，最后一笔交易的发起方可以赢得奖池中所有的代币

getCurrentRoundInfo()降低攻击成本。

https://medium.com/coinmonks/how-the-winner-got-fomo3d-prize-a-detailed-explanation-b30a69b7813f

重入蜜罐 地址映射 Address mapping

```
vulContract.call(bytes4(sha3("withdrawAll()")));
```



Call HelloWorld()

Found HW() on C, calling

HelloWorld() gets called

Call HelloMoon()

Found XX, calling

HelloMoon() never gets called

XX gets called

https://www.reddit.com/r/ethdev/comments/6n6t9w/function_hash_collision_potential_misuse/

withdraw(uint256) OwnerTransferV7b711143(uint256)

从新出发?

- 1 数据格式&地址格式 SafeMath / Complier level protection
- 2 完整校验&纠错 Pseudo level active check
- 3 收信应答 eg. “Unchecked CALL Return Values”
- 4 超时&重试
- 5 数据流方向
- 6 流程顺序控制 Modifiers / External calls
- 7 分片控制 Racing
- 8 地址映射&路由 Function hash collisions

https://blog.sigmaprime.io/solidity-security.html

谢谢

https://chaitin.cn