



ISC 互联网安全大会



360 互联网安全中心

区块链系统中的攻击与安全防护

赵 赫

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China

关于我



ISC 互联网安全大会



360 互联网安全中心

赵赫 (钟隐) Eric Zhao
ZHAOH@HFCAS.AC.CN

中国科学技术大学 博士

中科院合肥研究院 高级工程师

中科智链 联合创始人、CTO

巴比特区块链版主

推特公众号cnLedger创办者

首批获国家基金资助开展区块链技术研究



ISC 互联网安全大会



360 互联网安全中心

为什么我们说 区块链很安全 ？

WEB INTERNET
INFORMATION LEAK
TECHNOLOGY
TERMINAL AGE
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

为什么我们说区块链很安全？



数据公开透明 & 身份隐私保密



记录不可篡改 & 交易无法抵赖



去中心化网络 & 分布式共识

“至2025年，全球GDP总量的10%，将在区块链上记录和交易。” — WEF 2017





ISC 互联网安全大会



360 互联网安全中心

为什么我们说 区块链还不是很安全 ？

WEB INTERNET
INFORMATION LEAK
TECHNOLOGY
TERMINAL AGE
PERSONAL PRIVACY IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

为什么我们说区块链还不是很安全？

区块链 的安全现状：**黑客的提款机**



= =



区块链系统中的攻击分类

(1) 应用层攻击： 钱包和智能合约



(2) 系统层攻击： 交易所和服务商



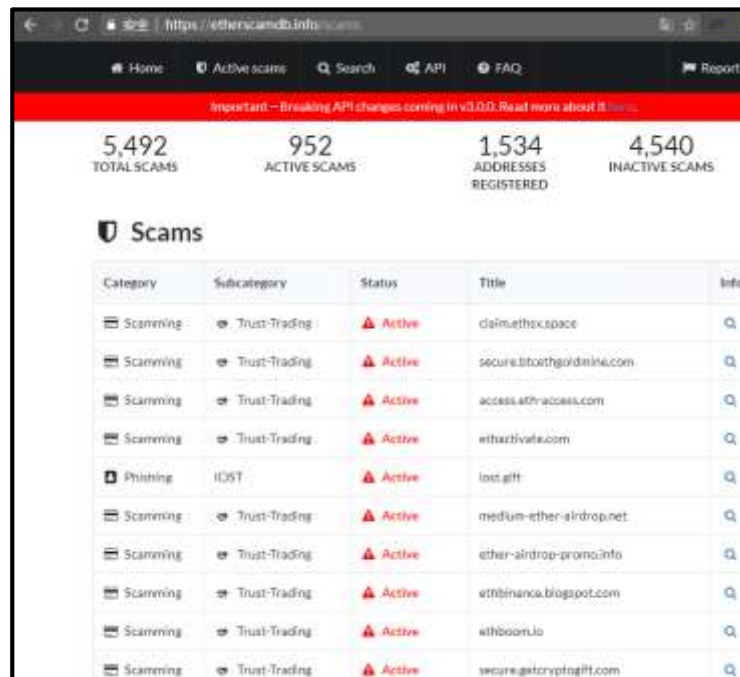
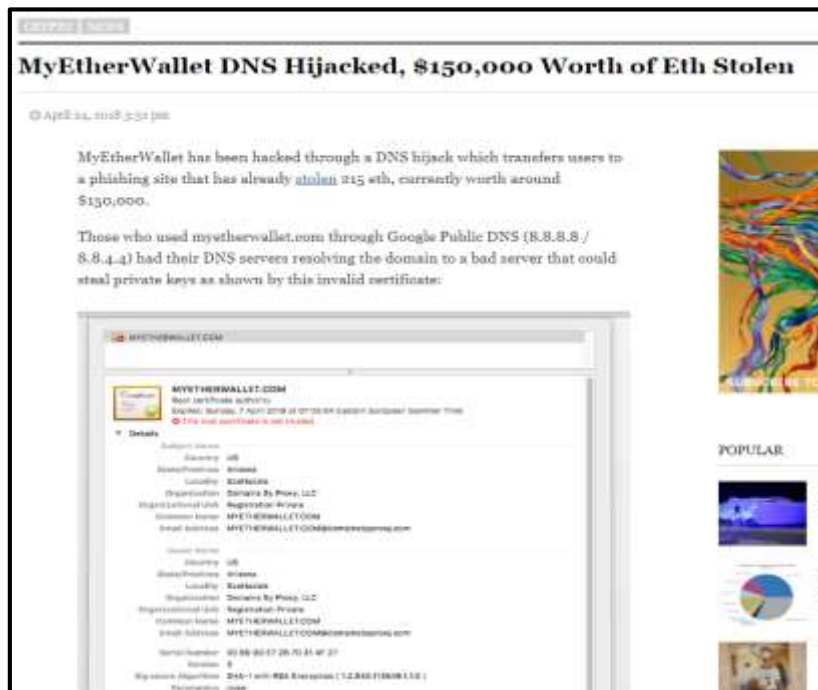
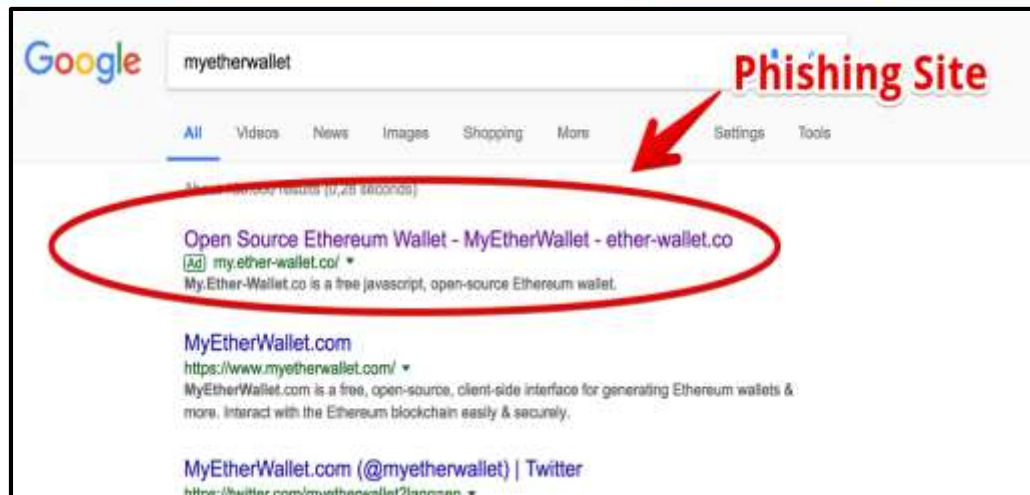
(3) 基础设施层攻击： 共识、算法、P2P网络



(1) 应用层攻击： 钱包和智能合约



案例：MyEtherWallet 在线钱包攻击



案例：本地PC钱包地址替换攻击

Qutra
Live Qutra / Project
Evrial

PROJECT
QUTRA
EVRIAL

0 posts
55 sympathies
1 month with us

1. The victim launches the EXE (which is being rebuilt in the web panel, which is activated by you after purchasing the product). It is written to the startup (Each time the PC starts, it launches the password stylus / cookie and the clipper operation).

2. Project Evrial expects any change to the clipboard, and if it determines that the clipboard contains a supported format, makes a request for a secure web connection to the web panel, gets what it needs to replace and makes a replacement.

3. The Web panel displays that the clipboard has changed.

4. Despite waiting for the change of the clipboard, a zip file from the stylus is sent to the web panel (Desktop screen, desktop files, passwords, cookies) and it is also displayed in it.

Spoiler: Programs supported stylus | Replacing wallets.

Clipper:

BTC, LTC, MONERO, ETHEREUM
QW, WMR, WMZ, WME
Steam Trade Offer Link

Stealer:

Supported browsers:
Chromium (Passwords + Cookies)
Google Chrome (Passwords + Cookies)
Opera (Passwords + Cookies)
Kometa (Passwords + Cookies)
Amigo (Passwords + Cookies)
Orbitum (Passwords + Cookies)
Orbitum (Passwords + Cookies), (the cookies have)
Camodo Dragon (+ Passwords, the cookies have)
Vandex Browser (Passwords, the cookies have +)

Supported utilities:

FileZilla
the Pidgin

Supported Stiller file formats from your desktop:

doc all
docx
txt
the log

Screenshot desktop

For all those who bought it - free updates!

The price at the moment is: 1500 RUB | \$ 27 | 30 \$ BTC
My contacts: Telegram

```
if ( GetTheClipboardData(&String) )
{
    if ( lstrlenA(&String) > 40 && lstrlenA(&String) < 50 && String == '0' && v7 == 'x' )
    {
        v2 = 0;
        for ( i = 0;
            *(&String + i) >= 97 && *(&String + i) <= 122
            || *(&String + i) >= 65 && *(&String + i) <= 90
            || *(&String + i) >= 48 && *(&String + i) <= 57;
            ++i )
        {
            ++v2;
        }
        if ( v2 == 42 )
        {
            lstrcpyA(&String1, "0x004D3416DA40338FAF9E772388A93FAF5059bFd5");
            v14 = 49;
            SetTheClipboardData(&String1);
        }
    }
}
```

Transactions

Token Transfers

Comments

17 Latest 25 txns from a total Of 40 transactions

TxHash	Block	Age	From	To	Value
0x7636dd57f9db634	5776519	17 hrs 16 mins ago	0x001d3416da4033	OUT	0x6edc4a5b9539825 2.3 Ether
0x9390984afbb35dc	5776258	19 hrs 41 mins ago	0x001d3416da4033	OUT	0xae68ca38b502e98 3 Ether
0xdda4db3621fa07b	5775304	22 hrs 52 mins ago	0x001d3416da4033	OUT	0x2d4556f945b6226 3.89 Ether
0x4832fc4bc319460	5775099	23 hrs 43 mins ago	0x001d3416da4033	OUT	0xb3c7c845da0ee3 3 Ether
0xe5c7775a5c36844	5774712	1 day 1 hr ago	0x001d3416da4033	OUT	0xa35468afdbcb111 1 Ether
0e565d7be900ee0a	5768333	2 days 4 hrs ago	0x817541c71c7779	IN	0x001d3416da4033 0.0005 Ether
0xb406519b161205	5762974	3 days 3 hrs ago	0x0626bd344d1222f	IN	0x001d3416da4033 0.127 Ether
0x44332bdde7956e	5760061	3 days 15 hrs ago	0x5a24bd380513e3	IN	0x001d3416da4033 0 Ether
0x866d89b80a5d79	5760053	3 days 15 hrs ago	0x64bec727099b03	IN	0x001d3416da4033 0 Ether
0xcdb1815b1519a4c	5750719	5 days 7 hrs ago	0xbwacalla8cha093	IN	0x001d3416da4033 0 Ether
0x8bb1c8b74a1714db	5729495	9 days 1 hr ago	Coinbase	IN	0x001d3416da4033 1.01 Ether
0x171cc150b120519	5729919	10 days 16 hrs ago	0x4c09db79117dbcf	IN	0x001d3416da4033 0.016 Ether

案例：社会工程学 & 手机/邮箱攻击

2016年12月，黑客通过攻击区块链VC投资人沈波 (Bo Shen)的手机，成功窃取大量ETH币和Augur币，造成至少\$300,000的损失。



案例：著名的智能合约攻击事件

- 2016年，黑客攻击DAO智能合约，成功盗取360万个ETH（现在相当于72亿元）
- 2017年，Parity多重签名合约存在漏洞，被两次攻击，先后造成15.3万个ETH、93万个ETH的损失
- 2018年4月，美链BEC出现合约无限复制token的Bug，市值蒸发64亿
- 2018年7月，Bancor智能合约更新程序遭黑客攻击，损失约2.5万个ETH和一些其他加密货币

“(Not So) Smart Contract”

...



(2) 系统层攻击： 交易所和服务商



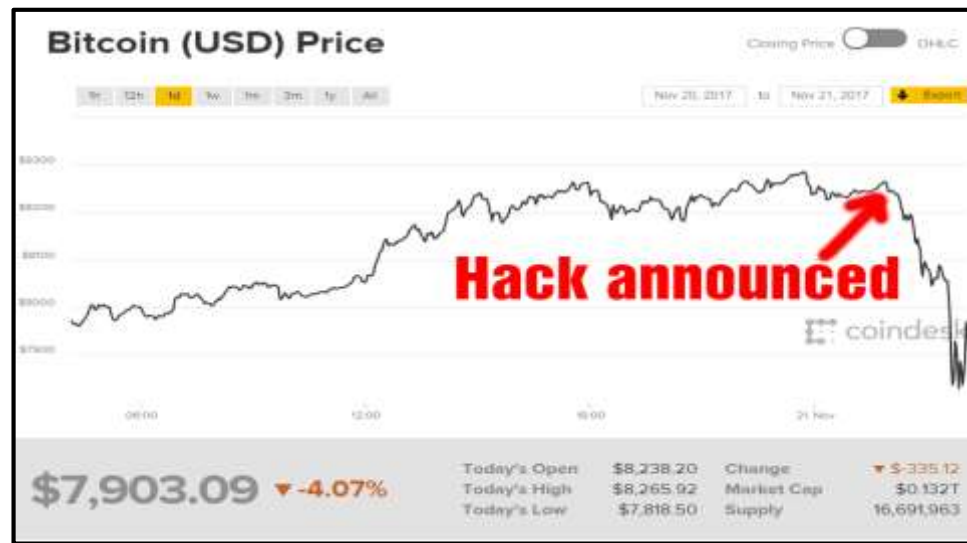
案例：加密货币交易所屡遭攻击

- 服务器被攻破
 - Bitfinex, Poloniex, Bithumb, Youbit, CoinCheck, GateCoin, Bitcoinica, BitGrail ...
- 监守自盗（内鬼作案 or 跑路）
 - Mt. Gox, ShapeShift, CoinSecure, Bit LC, Bitcoin7, ...
- 区块链底层Bug被利用
 - Coinbase, Mt. Gox, ...



案例：一些加密货币在线服务商的典型安全事故

- 针对服务器软件的攻击
 - Tether (USDT)
 - Blockchain.info
 - CoinDash ICO
 - Steem.it (STEEM)
- 针对管理人员的攻击(钓鱼)
 - BitPay
- 针对云服务器提供商的攻击
 - Slush Pool



(3) 基础设施层攻击： 共识、算法、P2P网络



案例：比特币 “1 RETURN” Bug（核心代码缺陷）

- 2010年7月，德国程序员ArtForz发现比特币脚本程序中有一处潜在破坏力极强的Bug
- **该Bug被恶意用户利用后，可以越权动用他人钱包中比特币，从而可能导致比特币变得一文不值**
- 比特币的创始人中本聪在邮件中给加文说（加文是比特币早期的另一位主要开发者，中本聪消失后接手比特币代码管理权）：

“对于其他不知道该 Bug 的人，要避免描述这个 Bug 的名字 (1 Return)”

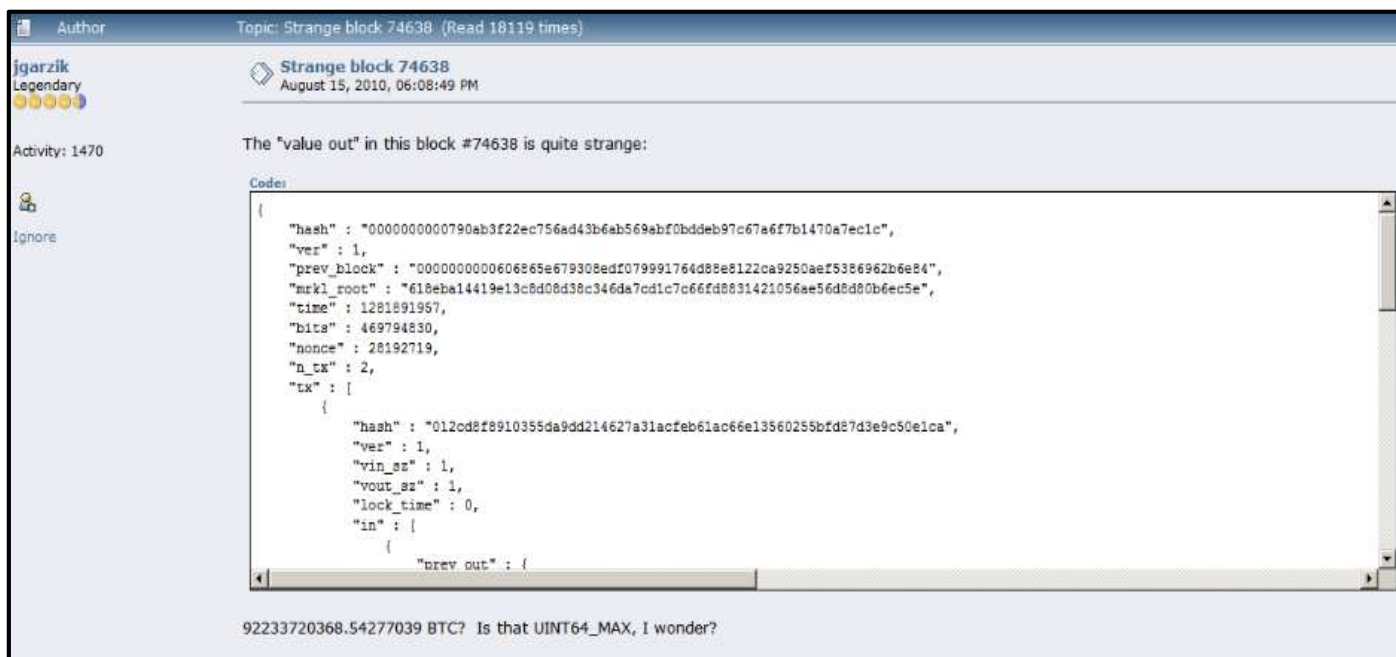
- **该Bug在大多数比特币节点经过更新修复、不再受此问题影响后，才被公之于众**
- 程序员ArtForz在发现Bug后选择悄悄告诉中本聪，成为比特币区块链历史上鲜为人知的安全救星

```
case OP_RETURN:
{
    pc = pend;
}
break;
```

OP_1 OP_RETURN

案例：比特币天量刷币漏洞（核心代码缺陷）

- 2010年8月，美国程序员Jeff Garzik发现比特币区块链中第#74638个区块，包含了一笔涉及3个地址、金额超过1800亿BTC的交易
- 经核实，**代码中检查交易的逻辑存在求和溢出漏洞，而未被妥善处理**
- 发现此Bug后，比特币开发者很快发布了含有补丁的新版本软件
- 在第#74691块，**带补丁版本的比特币区块链的长度终于追赶上并且超越了包含天量BTC漏洞的链**，最终是有惊无险地解决了这次比特币区块链历史上最为重大的危机事件。



The screenshot shows a forum post by user 'jgarzik' (Legendary) titled 'Strange block 74638'. The post is dated August 15, 2010, at 06:08:49 PM. The text of the post states: 'The "value out" in this block #74638 is quite strange:'. Below this text is a code block containing a JSON object representing a Bitcoin block. The JSON object includes fields for 'hash', 'ver', 'prev_block', 'mrkl_root', 'time', 'bits', 'nonce', 'n_tx', and 'tx'. The 'tx' field is an array containing a single transaction object. The transaction object has fields for 'hash', 'ver', 'vin_sz', 'vout_sz', 'lock_time', and 'in'. The 'in' field is an array containing a single object with a 'prev_out' field. The 'prev_out' field is an object with a 'hash' field. The 'hash' field contains a long hexadecimal string. The post also includes a comment at the bottom: '92233720368.54277039 BTC? Is that UINT64_MAX, I wonder?'

```
{
  "hash": "000000000790ab3f22ec756ad43b6ab569ebf0bddeb97c67a6f7b1470a7ec1c",
  "ver": 1,
  "prev_block": "0000000000606865e679308edf079991764d88e8122ca9250aef5386962b6e84",
  "mrkl_root": "618eba14419e13c8d08d38c346da7cd1c7c66fd8831421056ae56d8d80b6ec5e",
  "time": 1281891957,
  "bits": 469794830,
  "nonce": 28192719,
  "n_tx": 2,
  "tx": [
    {
      "hash": "012cd8f8910355da9dd214627a31acfeb61ac66e13560255bfd87d3e9c50e1ca",
      "ver": 1,
      "vin_sz": 1,
      "vout_sz": 1,
      "lock_time": 0,
      "in": [
        {
          "prev_out": {
```

92233720368.54277039 BTC? Is that UINT64_MAX, I wonder?

案例：51%/双花 攻击（共识机制攻击）

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network.

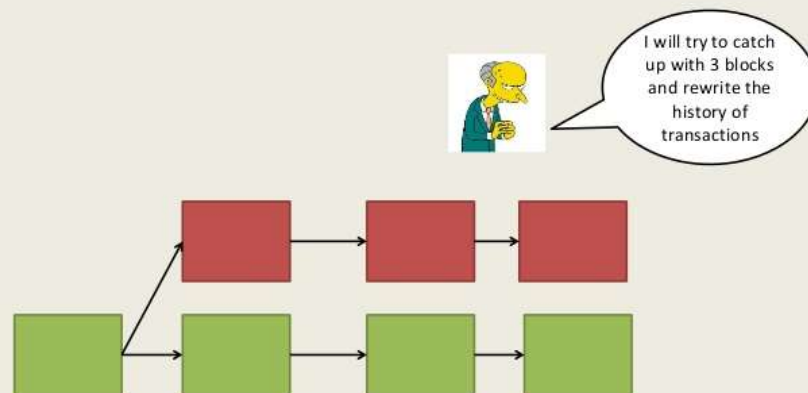
The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions,

We propose a solution to the double-spending problem using a peer-to-peer network.

51% attack [Nakamoto2008]



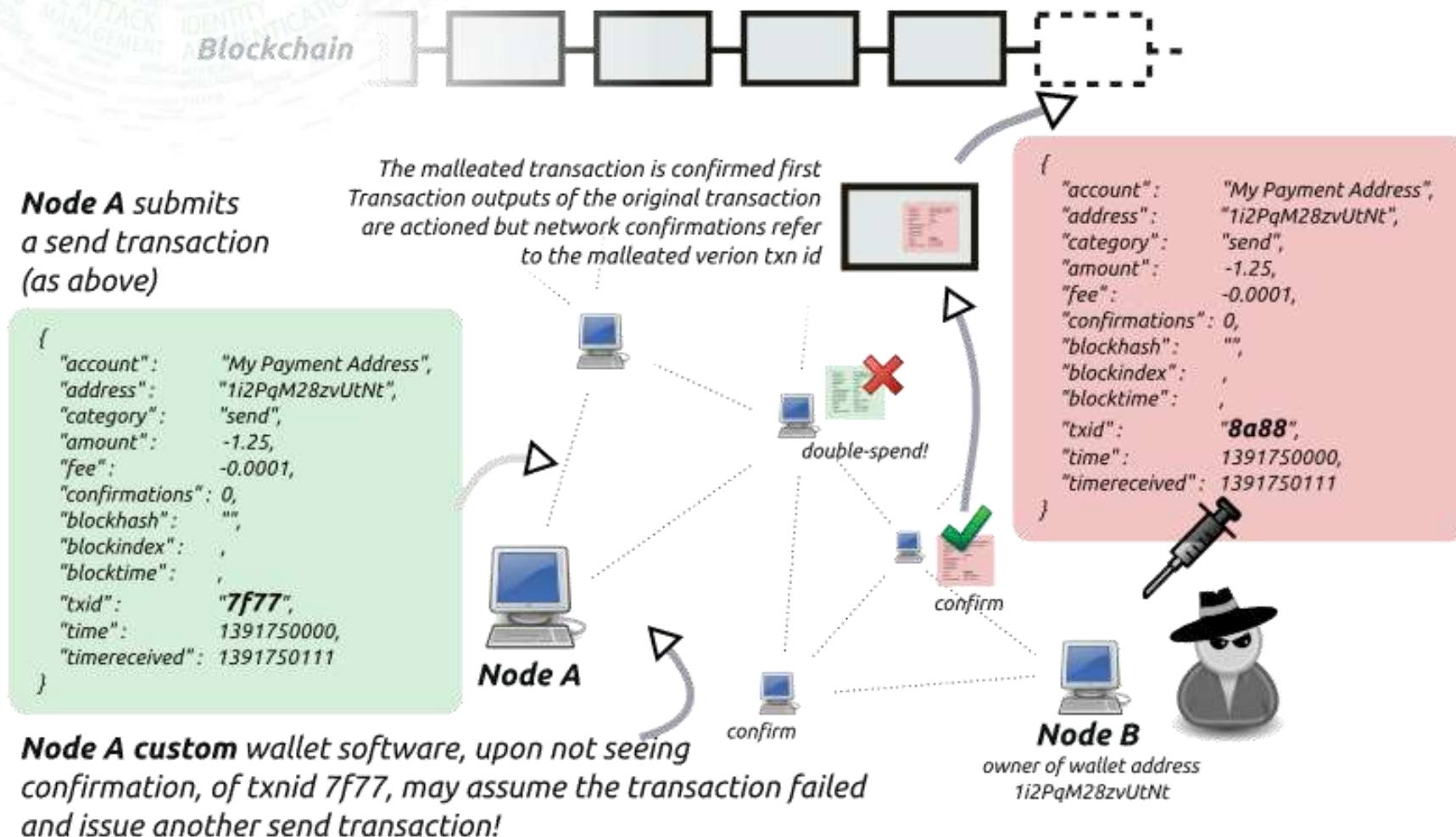
案例：双花攻击（共识机制攻击）

- BitcoinGold
 - 2018年5月，损失1.3亿元
- ZenCash
 - 2018年6月，损失340万元
- Verge
 - 2018年4月、5月，损失1900万元
- Monacoin
 - 2018年5月，损失62万元
- LitecoinCash, Krypton, Shift ...
- Who will be next?
 - 有学者的研究表明，
ETC: \$5千万 攻击成本 -> \$10亿 收益

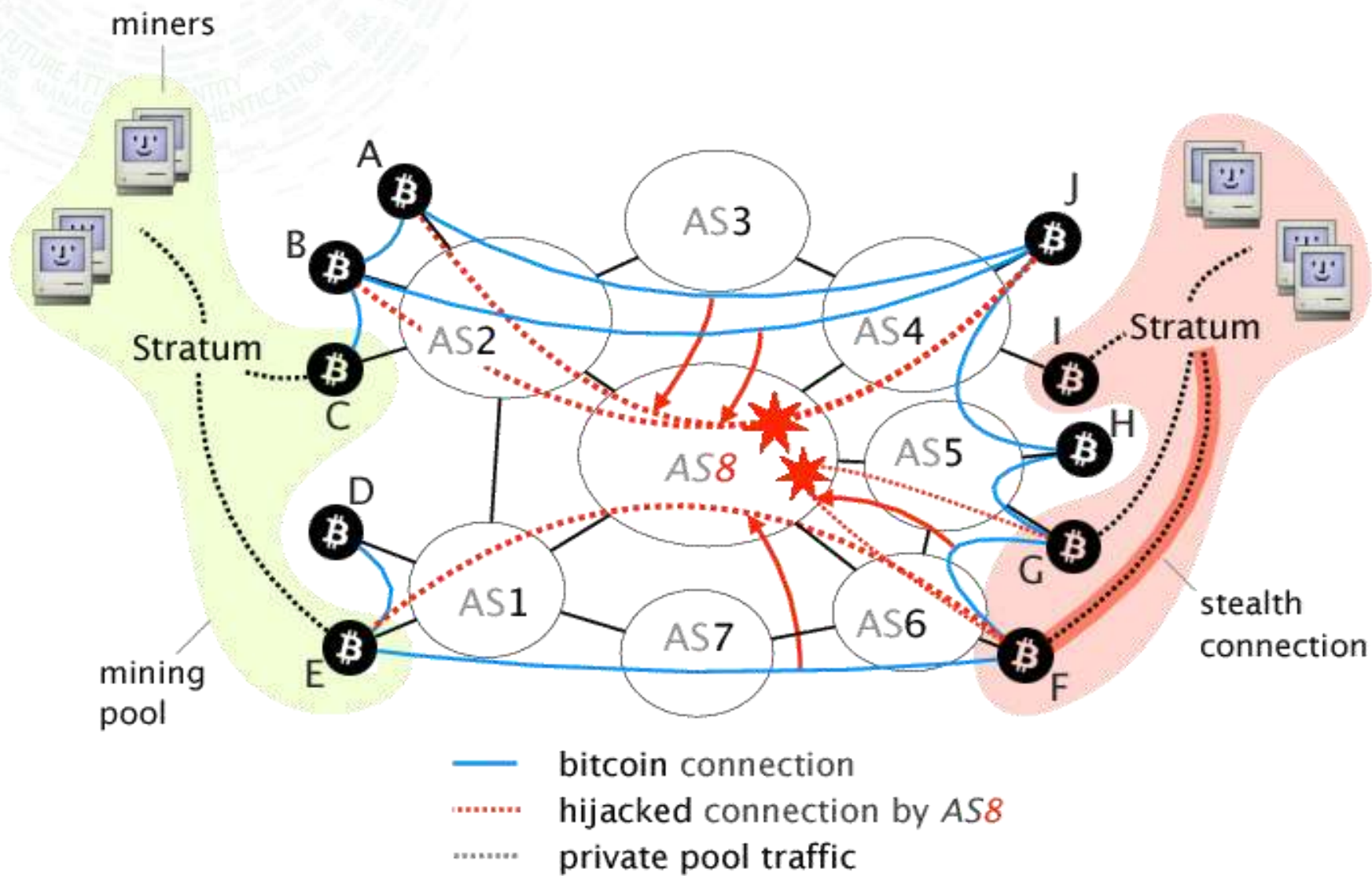


案例：交易延展性攻击（基础协议缺陷）

Malleated Transaction ID injection



案例：日蚀攻击（网络通讯漏洞）



案例：IOTA哈希冲突漏洞（加密算法漏洞）

- 2017年5月，IOTA团队请求MIT的研究组审计其软件及代码
- 7月，MIT研究者告知IOTA团队，他们发现了IOTA的加密哈希功能函数Curl中存在严重的漏洞（哈希碰撞），因此IOTA的数字签名及POW安全性均无法保障
- 8月，IOTA团队采用SHA-3替代掉了备受质疑的Curl哈希算法
- 9月，MIT研究者公布了之前发布的漏洞审查报告。IOTA团队随即强烈抗议，认为MIT人员违反学术道德，并声称：

“之前MIT学者发现的所谓的漏洞，实际上是我们有意为之，目的是防止代码被他人抄袭拷贝。”

IOTA Vulnerability Report: Cryptanalysis of the Curl Hash Function Enabling Practical Signature Forgery Attacks on the IOTA Cryptocurrency

By Ethan Heilman (Boston University, Paragon Foundation, Commonwealth Crypto), Neha Narula (MIT Media Lab), Thaddeus Dryja (MIT Media Lab, Lightning Network Dev), Madars Virza (MIT Media Lab, Zcash)

Team contact e-mail: curl@mit.edu

Summary: We present attacks on the cryptography used in the IOTA blockchain including under certain conditions the ability to forge signatures. We have developed practical attacks on IOTA's cryptographic hash function Curl, allowing us to quickly generate short colliding messages. These collisions work even for messages of the same length. Exploiting these weaknesses in Curl, we break the EU-CMA security of the IOTA signature scheme. Finally we show that in a chosen message setting we can forge signatures of valid spending transactions (called bundles in IOTA). We present and demonstrate a practical attack (achievable in a few minutes) whereby an attacker could forge a signature on an IOTA payment, and potentially use this forged signature to steal funds from another IOTA user. This report provides example demonstrations of these vulnerabilities but does not detail the exact cryptanalytic process to generate the collisions. A later publication will provide an in-depth study of our cryptanalysis of Curl.



IOTA :



案例：IOTA缠结缝合攻击（共识机制攻击）

The Tangle main net

Switch network: [main](#) [test](#) [spam](#)

- ☒ tip
- ☐ milestone
- ☐ transaction
- ☐ confirmed

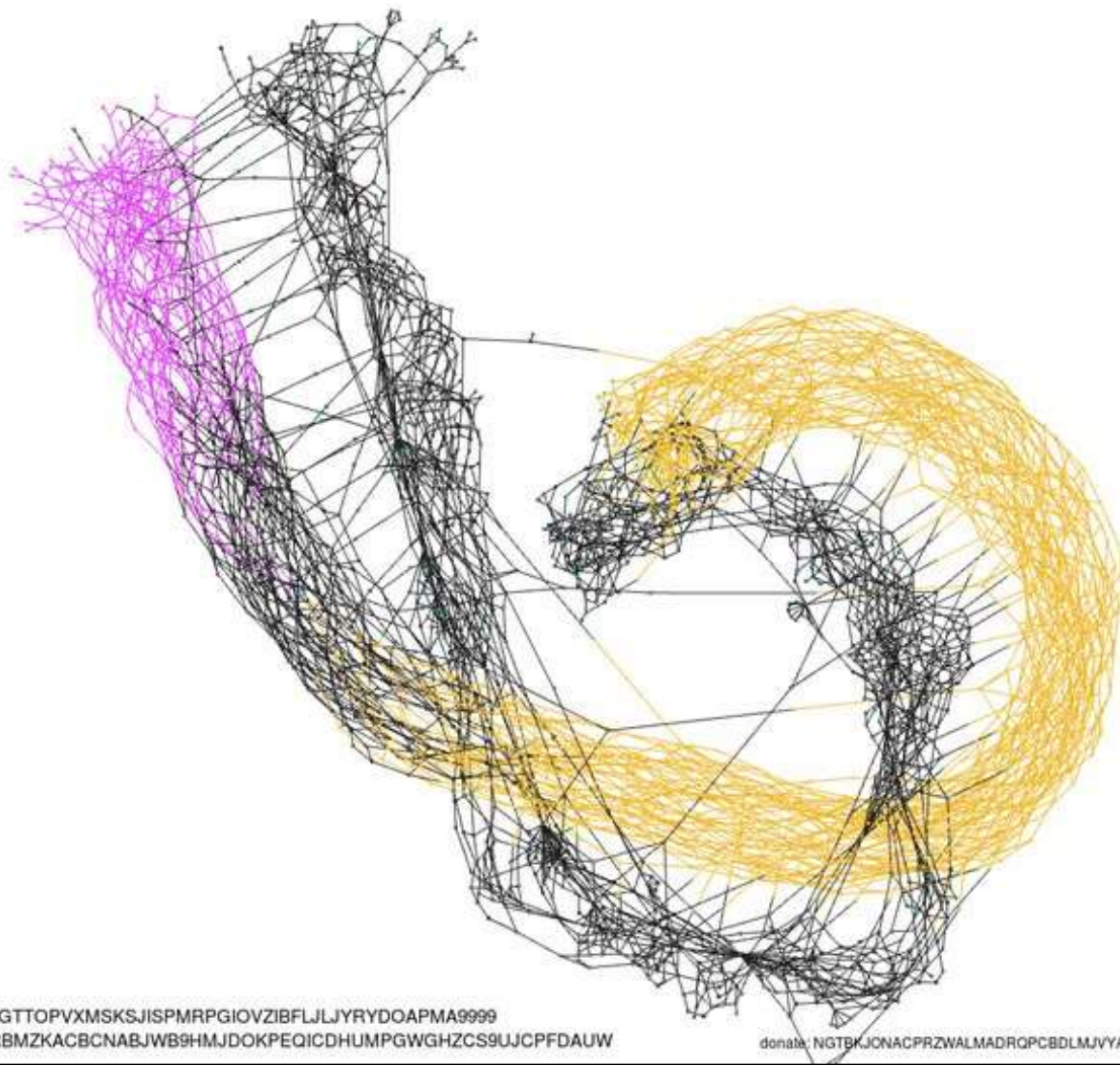
select a transaction to view

- ☒ 362 confirmed by tx
- ☐ 1375 confirming tx
- ☐ same bundle

enter a tx hash

enter a tag

enter a bundle-hash



- ☒ remove floating tx
- ☐ limit to 4k tx
- ☒ pin old tx
- ☐ reduce movement
- ☐ size by # of confirms
- ☐ size by weight
- ☐ size by value
- ☐ color by order
- ☐ lighten links
- ☐ dark mode

hide



Donations

donate

300.00Mi

1.00Mi hsnj8oz

500.00ki hsnj8oz

101.00ki hsnj8oz

tips ratio: 9.46%

confirmed ratio: 0.20%

(30s avg) tps: 4.97

transactions: 3504

(301.794Mi)

value: 0.00i

tx tag: SIDETANGLE9ROCKS999999999999

tx hash: LEFQD9Z9OKHCSIV9WKVRYPAFUFHYXMUQUDJWPNGTTPVXMSKSJISPMRPGIOVZIBFLJLJYRYDOAPMA9999

bundle hash (0/0): HZELRVGIWETDSHRIOWFIRPNCMPIFDTHRBZKACBCNABJWB9HMDOKPEQICDHUMPGWGHZCS9UJCPFDAUW

donate: NGTBKJONACPRZWALMADROPCBDLMJVYAIHBLQ9QIDLYSFRFIE9NCM9QSYTZQDRPCTVEZE9KVWOOHLBFHBBPUCLJU9 (301.794Mi)

问题：区块链技术重新定义了安全吗？

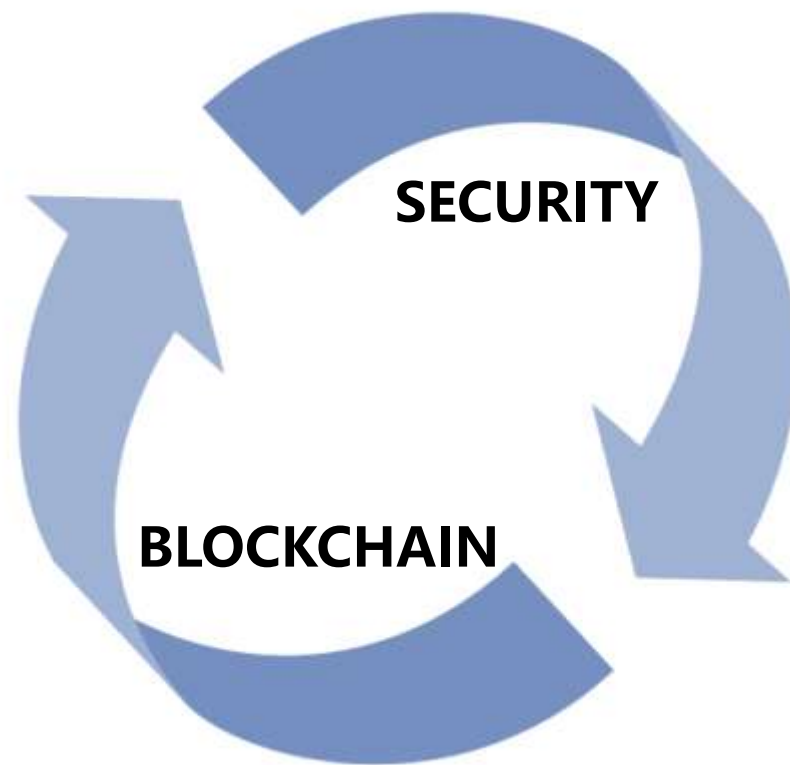
- 区块链技术 **不是** 安全的万能药

区块链系统中仍会继承现有的互联网安全问题、软件安全问题，同时还会引入新的攻击向量。

- 但是，区块链系统能够在下述方面 **显著提升** 安全性：

- 1、容忍部分节点作恶，而不影响系统整体安全
- 2、没有“单点失败”

- 前提：**在区块链系统的设计、研发和运营中，对于安全问题充分重视、做好防范**





ISC 互联网安全大会



360 互联网安全中心

关于区块链系统安全防护的一些建议

WEB INTERNET
INFORMATION LEAK
TERMINAL AGE
PERSONAL PRIVACY
IDENTITY SECURITY
IDENTITY
AUTHENTICATION
ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
INDUSTRIAL

如果你是一位区块链资产的 持有者（用户）：

- 牢记：私钥即权利
- “买买提”
- 不要重复使用密码，使用自动生成的密码
- 开启2FA
- 从收藏夹访问交易所、检查SSL标志。
学会识别并避免百度、谷歌等的推广链接
- 仔细阅读产品或网站上的“安全提示”相关内容
- 大额资产离线存储，或使用知名厂商的硬件钱包
- 慎用云盘、云笔记软件等备份私钥数据
- 保管好您的邮箱账号
- 建议使用苹果手机（我也很喜欢安卓，但大多数安卓手机的安全更新不及时）



Bitcoin – The Halving by Crypto Art

如果你是一位区块链项目的 开发者：

- Don't Trust. Verify!
- 习惯“去中心化”思维，您面对的是拜占庭节点
- 不要尝试使用自己发明的加密算法
- 谨慎对待随机数
- 不要轻信时间戳
- 重视安全测试用例的编写，在开发时即充分开展安全测试
- 检视您引用的每一个Library
- 如果您的工作基于其他项目（如BTC/ETH），应关注并同步更新其漏洞补丁部分的代码
- 告诫自己写好智能合约很难，对合约安全检查应谨小慎微
- 补齐加密学和安全基础知识，并学会看论文
- 您开发的区块链系统有多安全，完全取决于您，而不是取决于高大上的“区块链技术”



Ethereum 'Abstractions' by Frankreddit5

如果你是一位区块链相关产品的 **创业者**：

- 如您的项目尚未开始：问一问自己，一定要用区块链吗？
- 如您的项目已经开始：重新从安全的角度审视它的各个方面
- 应充分了解：在安全上您将投资大量资源，但看不到短期回报；只有当安全事故出现的时候，才能知道代价有多么大
- 确保为用户提供了足够的安全提示和安全教育
- 防范针对自己以及关键团队成员（人）的安全攻击
- 修复服务器上非区块链系统（网站系统、操作系统等）的漏洞
- 划拨资金设立Bug Bounty；聘用安全顾问，请第三方审计代码
- 如果产品为公链，建议用两组人员、两种不同语言独立开发
- 开源的，才是安全的（但不要等到上线前一天才开源）
- 做好思想准备：系统一定有漏洞、一定会被攻破的。因此要有：安全专员、应急小组、安全预案



Strategy of Blockchain Painting by Daniel Loveday



ISC 互联网安全大会



360互联网安全中心

谢谢!

联系方式: zhaoh@hfcas.ac.cn

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing · China