

出其不意 攻其不备

——区块链别样攻击及应对

启明星辰 核研院研究二部总监

谢安明



目录

CONTENTS

01

区块链是什么

02

私钥碰撞

03

DDoS攻击

04

隐私挖掘

● “它是一台创造信任的机器！”

- 权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等——**区块链技术将影响世界！**
- 金融、物联网、供应链、公证
- 社区、联盟、初创、投资



你应该像对待90年代互联网那样认真对待这种技术。

——Blythe Masters, DAH

区块链是一个环环相扣的分布式计算系统

核心
技术

分布式账本

共识机制

密码技术

智能合约

区块链是一个**分布式账本**，一种通过**去中心化**、**去信任**的方式集体维护一个可靠数据库的技术方案。

- 跨境支付
- 加密货币

数字货币



- 电子票据
- 证券发行
- 供应链金融
- 物联网

数字资产



- 网络安全审计
- 企业/个人信用
- 身份/档案存证
- 数字版权管理

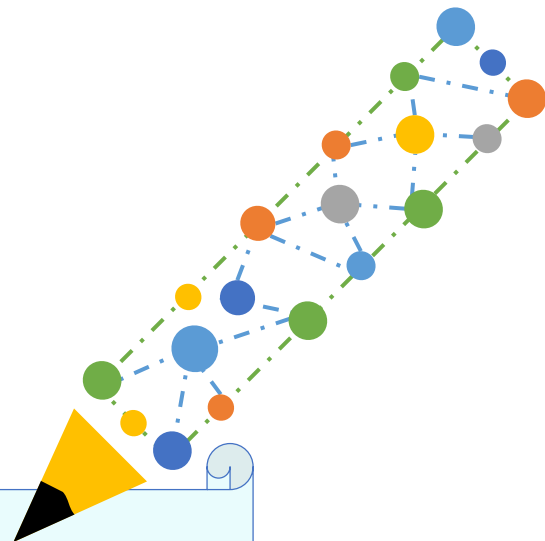
数字存证



2015年下半年开始，区块链技术迅速走红，应用领域不断扩展，从最初的数字货币延伸到金融，甚至社会各个领域，新一轮的科技新浪潮有望就此展开。

• 道高一尺，魔高一丈！

- 安全将成为区块链技术的最大挑战！
- 有可能严重阻碍区块链技术应用！



区块链应用安全事件

世界上最大的比特币交易所运营商Mt.Gox宣布其85万个比特币（约值4.73亿美元）被盗

2014年2月

香港数字货币交易所Gatecoin被黑，价值超过200万美元的以太坊相关资产被盗

2016年5月

CoinDash在首次发行代币（ICO）时受到攻击，收款地址被篡改，损失约700万美元

2017年7月

币安交易所受到攻击，攻击者操作币市，通过做空获利超过1亿美元

2018年3月

2015年2月

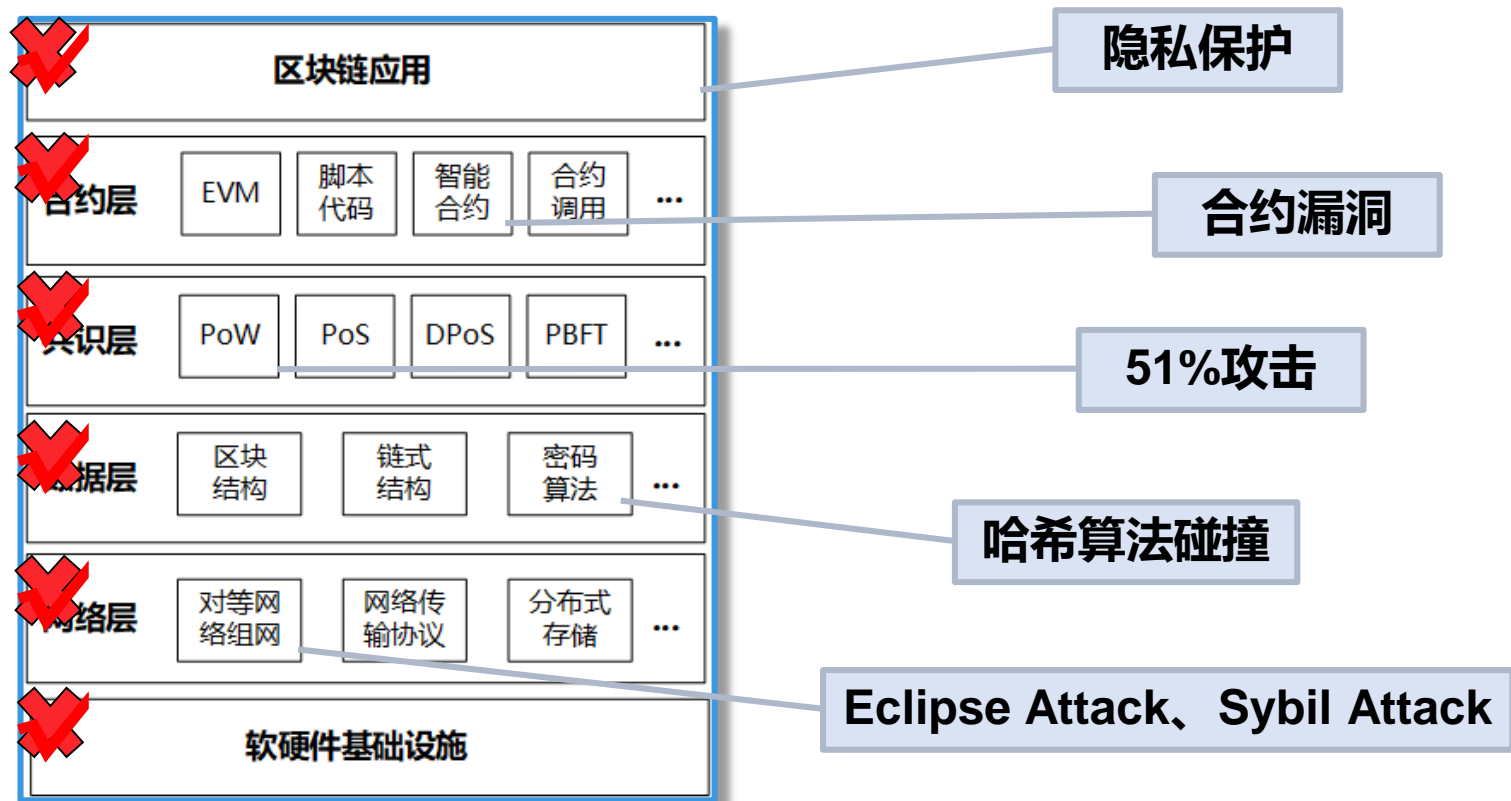
“比特币存钱罐”发表声明，其服务器被入侵，黑客从中盗取的比特币数量超过3000个，随后网站关闭

2016年6月

区块链项目The DAO遭受攻击，黑客利用The DAO程序中“递归调用漏洞”，成功盗取了360万枚以太币（约5000万美元）

2017年10月

比特币网络遭遇垃圾交易攻击，10%以上的比特币节点下线

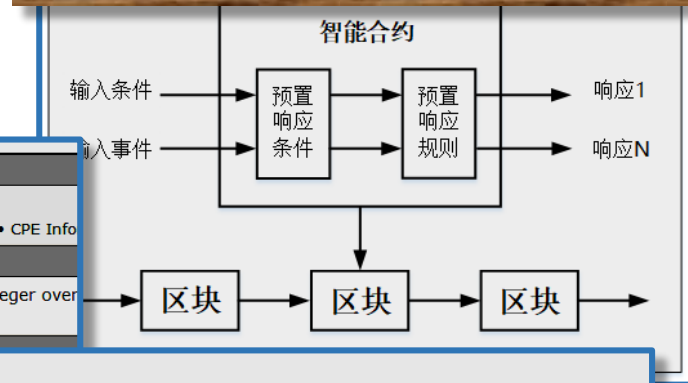


● 智能合约

■ smart contract

■ 一段写入区块链的代码

一个微小的代码缺陷，
可以产生灾难性的后果！



CVE-ID

CVE-2018-13041

[Learn more at National Vulnerability Database \(NVD\)](#)

• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Info

Description

The mint function of a smart contract implementation for Link Platform (LNK), an Ethereum ERC20 token, has an integer overflow vulnerability that allows an arbitrary user to mint any value.

References

Note: [References](#) are provided for the convenience of the reader to help distribute information.

- [MISC:https://github.com/dwfault/AirTokens/blob/master/Link_Platform/contracts/LinkToken.sol](https://github.com/dwfault/AirTokens/blob/master/Link_Platform/contracts/LinkToken.sol)

由计算机网络来执行

```
function mint(address _spender, uint _value)
    onlyOwner
    {
        balances[_spender] += _value;
        totalSupply += _value;
    }
```



目录

CONTENTS

01

区块链是什么

02

私钥碰撞

03

DDoS攻击

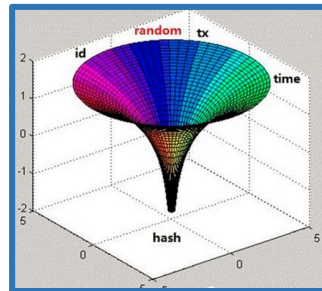
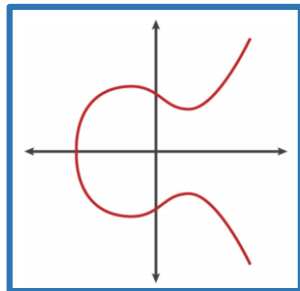
04

隐私挖掘

- 神话一：区块链私钥不可逆向，不可猜测！

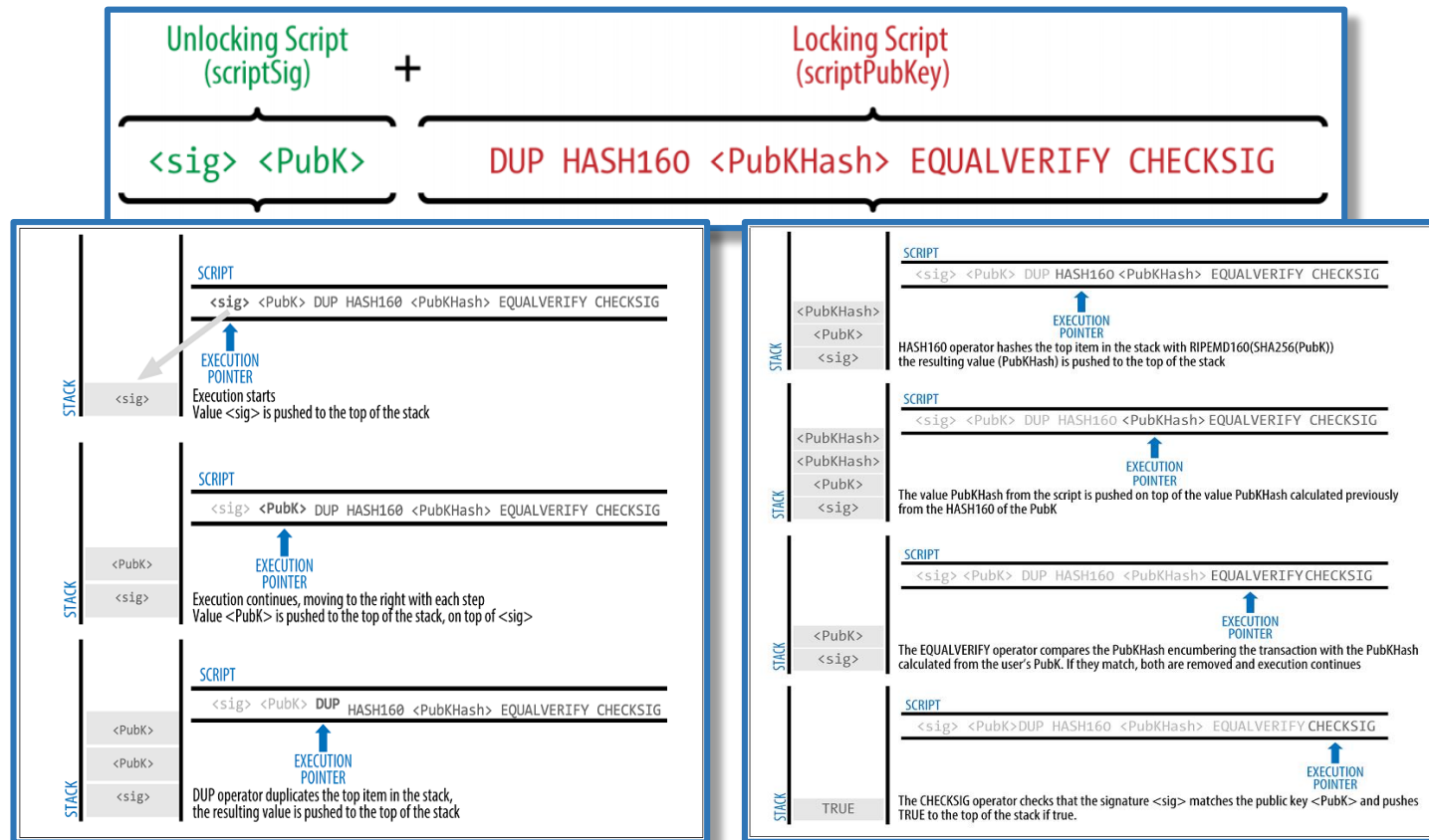


- 椭圆曲线
- 哈希算法
- Base58
- 脚本语言



Value	Character	Value	Character	Value	Character	Value	Character
0	1	1	2	2	3	3	4
4	5	5	6	6	7	7	8
8	9	9	A	10	B	11	C
12	D	13	E	14	F	15	G
16	H	17	J	18	K	19	L
20	M	21	N	22	P	23	Q
24	R	25	S	26	T	27	U
28	V	29	W	30	X	31	Y
32	Z	33	a	34	b	35	c
36	d	37	e	38	f	39	g
40	h	41	i	42	j	43	k
44	m	45	n	46	o	47	p
48	q	49	r	50	s	51	t
52	u	53	v	54	w	55	x
56	y	57	z				

P2PKH (Pay-to-Public-Key-Hash)



From: Andreas M. Antonopoulos, Mastering Bitcoin

- 不可能

- “ 2^{160} 的散列空间，也足够对抗HASH碰撞了！
- 假设用30EH/s的算力来碰撞，有效的地址10亿个
- $2^{160}/2^{65}/2^{30}=2^{65}$ ，换算成年大概是 10^{12} 年
- 假设宇宙年龄为100亿年， $10^{12}/10^{10}=100$
- 宇宙毁灭重生100次，我们有可能破解一个私钥！”

- 大型比特币地址对撞机

- Large Bitcoin Collider
- 猜测私钥

- 2016.04

- 项目开始运作，算力逐渐壮大到1GH/s的碰撞强度

- 16个

- 共发现了16个有效的私钥，其中有4个真实且有余额

- 共打捞了不到1个BTC

- 成本远超过所得

- “区块链安全牢不可破”

即便从 Internet Archive 等非营利机构抢夺一分一毛也会被视为不折不扣的混蛋。

Large Bitcoin Collider (2)

Page 1 out of 904625697166532776746648320380374280100293470930272690489102837043110636675 2.999 万亿个私钥

previous | next

Private Key	Address	Compressed Address
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreAnchuDf	1EHNa6Q4Jz2uvNExL497mE43ikXhwF6kZm	1BgGZ9tcN4m9KbZDn7KprQz87SZ26SAMH
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreAvUcVfH	1LagHjk2FyCV2ZrNHVqg3gY4TSYwDV4m	1cMh228HTCiwS8ZsaskH8A8wze1JR5ZsP
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreB1FQ8BZ	1NZUP3JA9JkmbvmoTv7nVgZGtyJirKV1	1CUNEBJYrCn2y1SdiUMohakUJ4wpP326Lb
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreB4AD8Yi	1MnyqgrXKmcWJHBYEsAW7oMlyqJAS81eC	1Jk9CQw1syRvJ1WtFMVomrYdV3W2tVBF9
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreB8for94	1E1NUNmYw1G5c3FKNP4d35QmDvuNG3auYk	17Vu7st1U1KwmyUKU4JlHeHHGRVNrqrLD
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreBKdE2NK	1UCZSVufT1PNimutbPdJuiEYCVSIZAD6n	1CF2hs39Voi6i1YNKYGUAcOhL2K2q4pawBq
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreBR6zCMU	1BYbgHp5KQCtMrQfWn6b6n5S718EJkEJ41	19ZewH8Kk1PDbsNjdJ97FP4EiCjTRaZMZQA
+ 5HpHagT65TZzG1PH3CSu63k8DbpvD8s5ip4nE83kEsreBbMaQXl	1JMcEcKXQ7xA7JLAMPsBmHz68bzugYtdrv	1EHqbyUMvvs7BFL8goY6qcPbD6YKfPqb7e

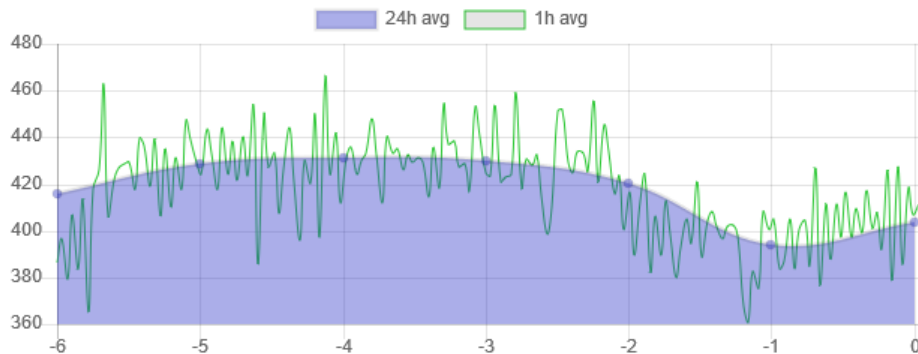
24h Pool Performance: 403.89 Mkeys/s

keys per day: 34.90 tn
total keys generated: 30831.43 tn
pages on [directory.io](#): 240870.55 bn
search space covered: 54.78 of 160 bits
search space in 1y: 55.27 bits



LBC Pot

0.13494528 BTC



- 保护私钥
 - 保护口令
 - 用健壮的钱包软件
- 使用多个账号
 - 不要把所有鸡蛋放在一个篮子里
- 使用新账号
 - 尽量保证每次使用新篮子
 - 每次支付时，将支付余额转到一个新的账户，废弃旧账户



目录

CONTENTS

01

区块链是什么

02

私钥碰撞

03

DDoS攻击

04

隐私挖掘

● 神话二：区块链技术天然可对抗DDoS攻击！

[区块链技术在物联网发展中扮演的新角色:抵御DDoS攻击 巴比特 服务...](#)



2017年2月27日 - 巴比特资讯, [区块链](#), [区块链技术在物联网发展中扮演的新角色:抵御DDoS攻击 区块链技术在物联网...](#)
www.8btc.com/blockchai... - 百度快照

[基于区块链的应用及网站如何抵御DDoS攻击 区块链 金色财经](#)



2017年6月26日 - 并且其数量攀升之快,极易成为DDoS攻击的目标,在这种情况下,[区块链](#)技术完全分布式的特性,就使得这项技术真正...
<https://www.jinse.com/news/blo...> - 百度快照

[为什么区块链技术是对抗DDoS攻击的最佳选择](#)

2017年10月1日 - 从房地产到数据服务,这些应用是[区块链](#)技术如何重塑数字信息展现的绝佳案例. 根据Inc的数据显示,[区块链](#)技术领域最近的发展可能会被用于终止DDoS(分布...
baijiahao.baidu.com/s?... - 百度快照

[为什么区块链技术是对抗ddos攻击的最佳选择 百度知道](#)

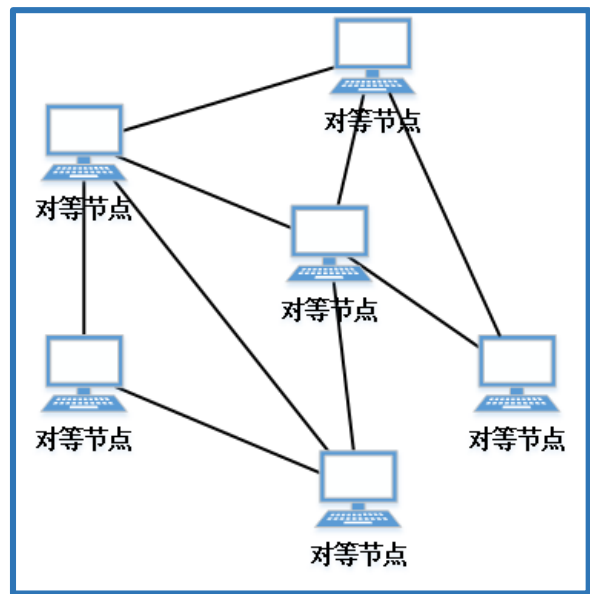
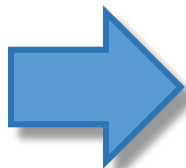
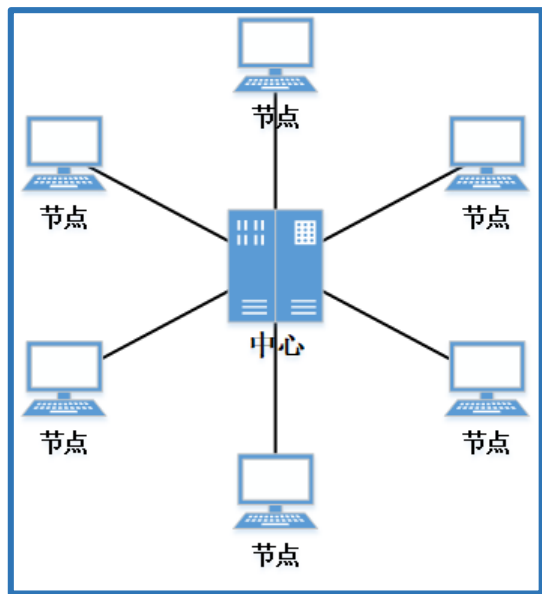
2017年10月5日 - 回答: 个人认为DDOS目前是无解的,没有什么最佳选择,只能被动防御,只是在遭攻击时尽量减小影响和损失,[区块链](#)技术和CDN类似,都是负载均衡的原理,只是具...
<https://zhidao.baidu.com/quest...> - 百度快照

[未来 区块链将是我们对抗黑客的最佳选择 - CSDN博客](#)

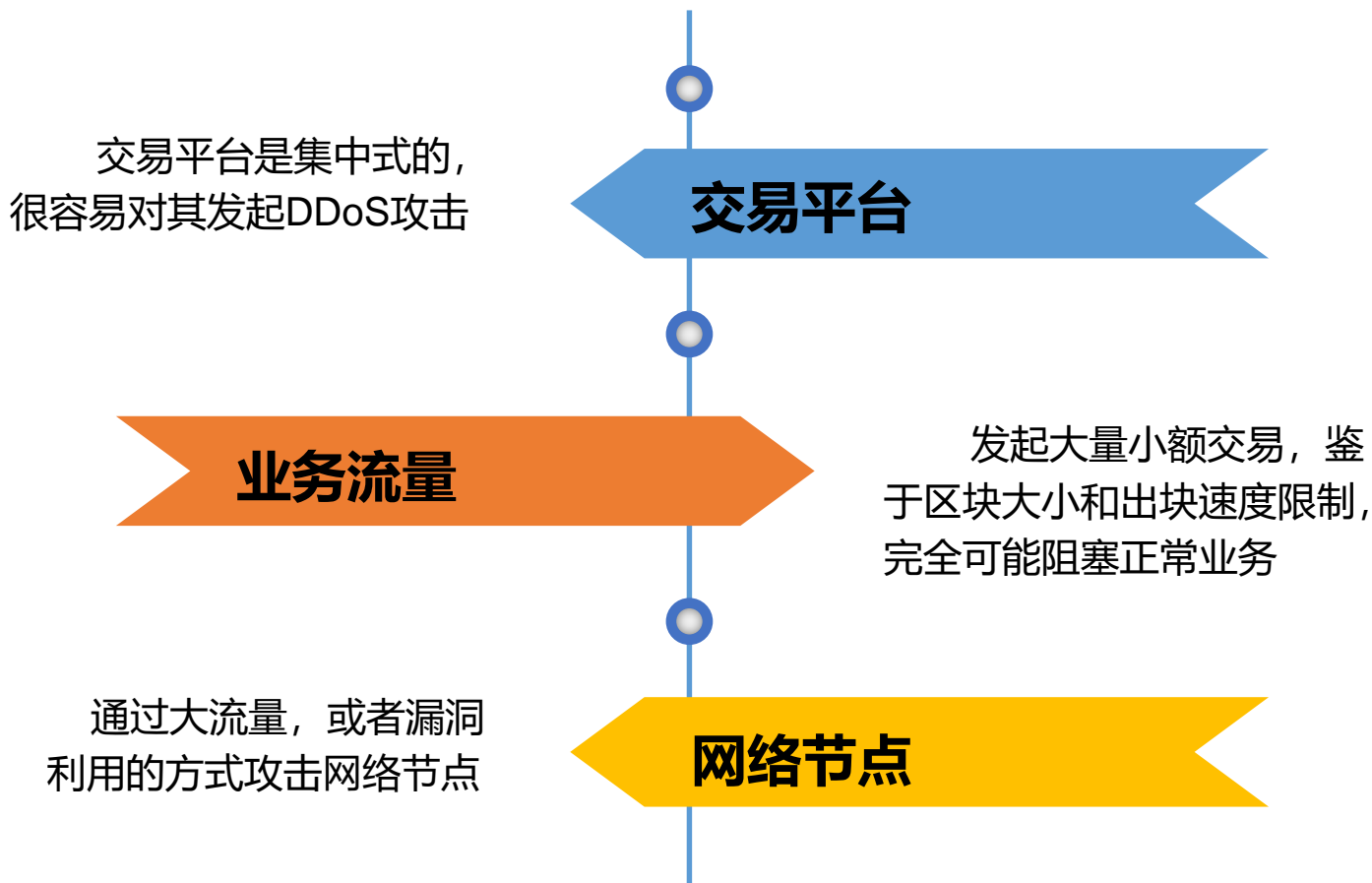


2018年2月5日 - 具体来看,[区块链](#)技术可以在管理和保护用户认证数据

区块链网络——分布式无中心网络



DDoS攻击是可能的



- 交易平台
 - 购买和出售加密货币中心
 - 集中式平台，成为“新中心”



Poloniex Exchange @Poloniex · 5月13日
We've been under continuous DDoS attack which inevitably affects other areas of operations. We're mitigating as fast as we can.

Poloniex Exchange @Poloniex · 5月12日
Severe DDoS; mitigating.

Poloniex Exchange @Poloniex · 5月9日
Coins are safe. We should be back up in about 15 minutes.

Poloniex Exchange @Poloniex · 5月9日
DDoS; we're working to mitigate.



遭

- 主链堵塞

- 短时间内交易量极大

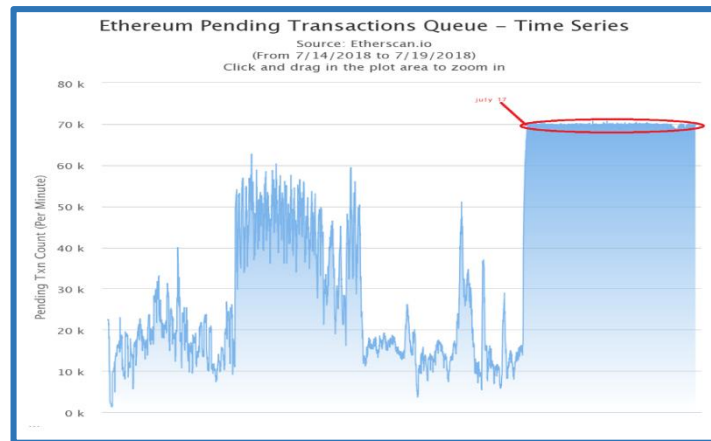
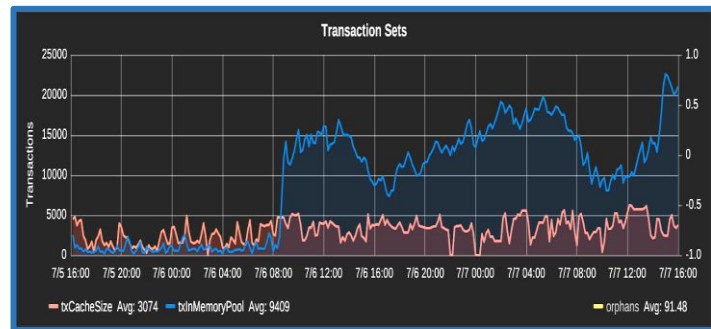
- ◆ 2017下半年，比特币垃圾交易

- ◆ 2017.12, CryptoKitties

- ◆ 2018.7, 以太坊拥堵

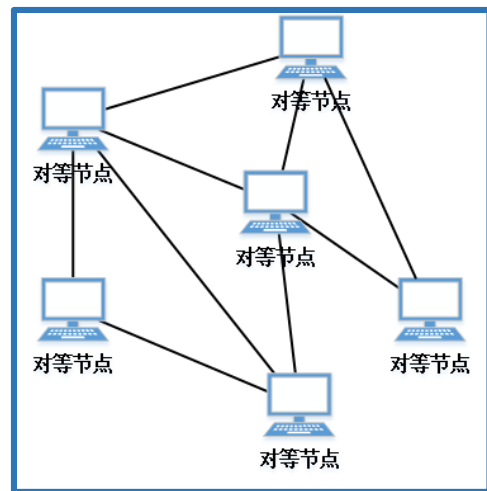
- 小额慢速交易

- ◆ 2016年以太坊, EXTCODESIZE

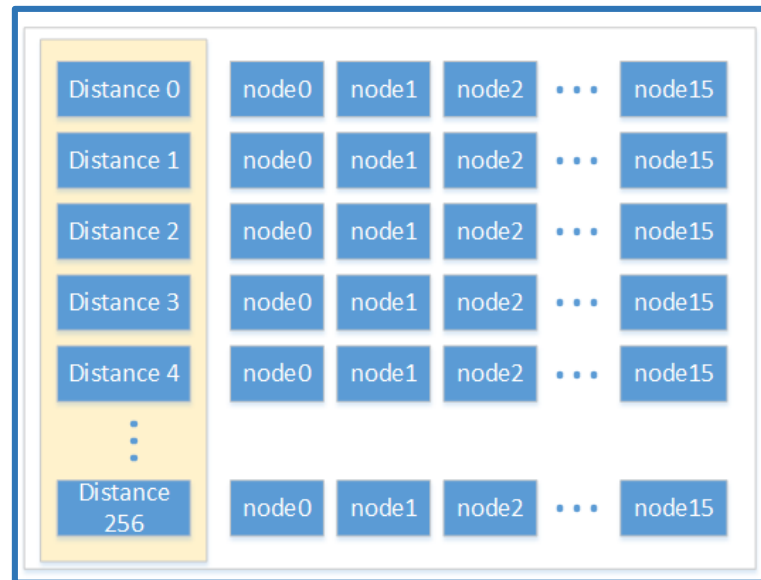
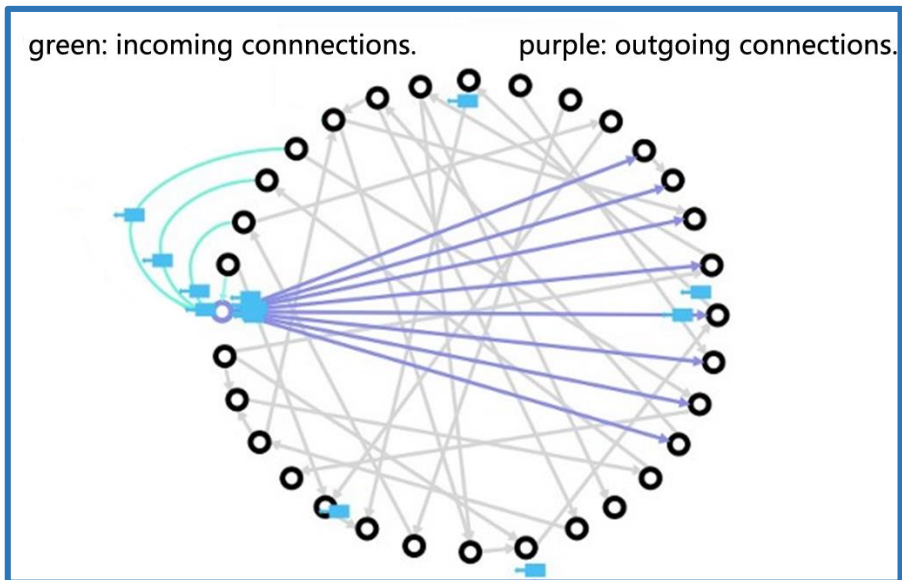


- 网络节点
 - 指定地址
 - 关键节点
 - ◆ 超级节点
 - ◆ CA/背书节点
- 闪电网络
 - 2018年3月
 - 接近20%节点被迫离线

- 区块链组网
 - P2P组网协议
 - 邻居发现协议
- 连接邻居
 - db 和 table
 - Maxpeers
 - ◆ Incoming、outgoing



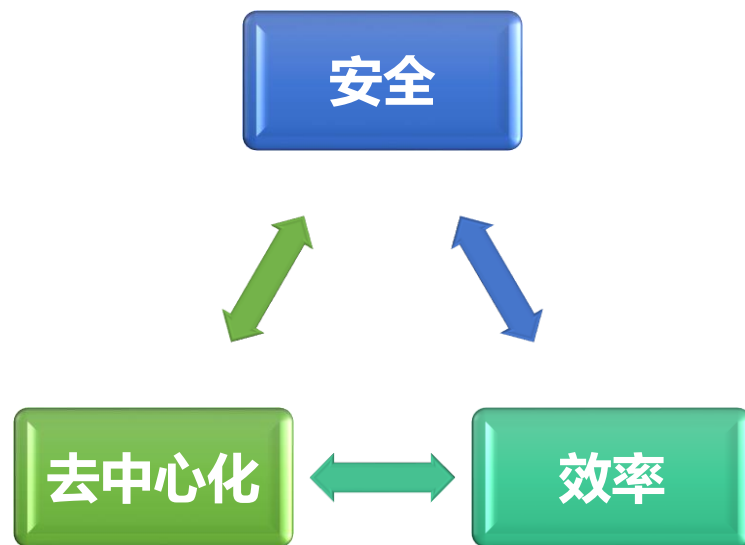
- 恶意填充节点的连接



- 防护对象
 - 交易平台
 - 网络节点
 - 业务流量
- 传统防DDoS机制
 - 扩充资源（带宽、服务器等）
 - 部署防护设备
 - 减少业务

- 区块链技术

- 提高收费价格
- 修补漏洞
- 修改共识机制、提高交易效率
- 侧链、扩容





目录

CONTENTS

01

区块链是什么

02

私钥碰撞

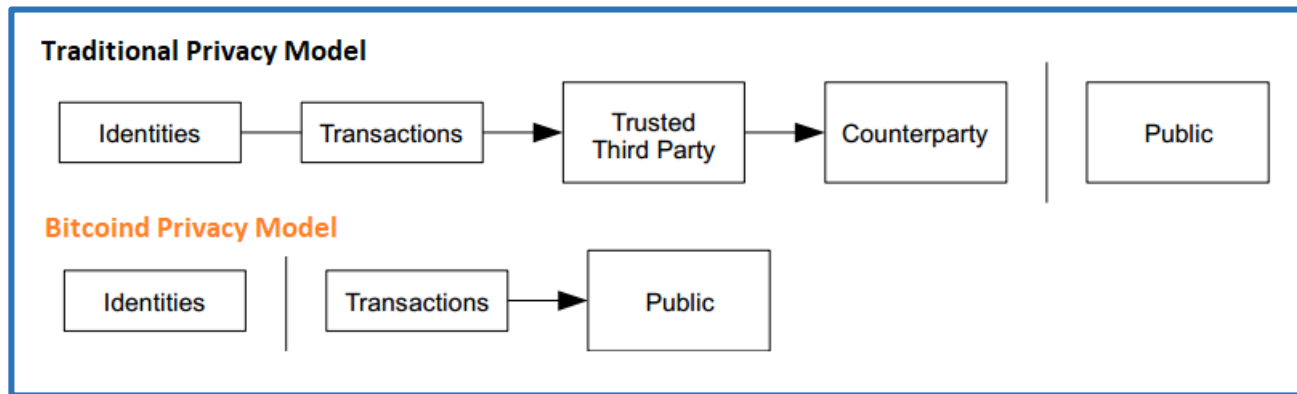
03

DDoS攻击

04

隐私挖掘

- 神话三：区块链是匿名的！



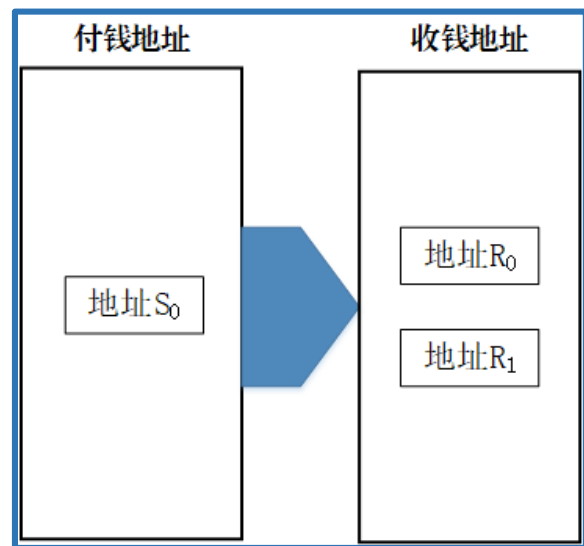
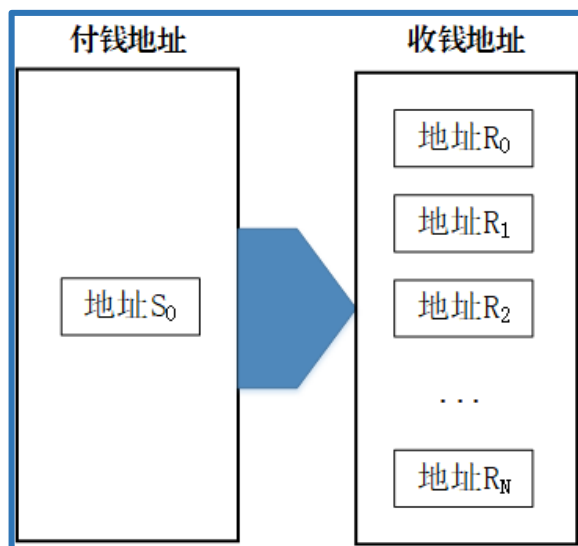
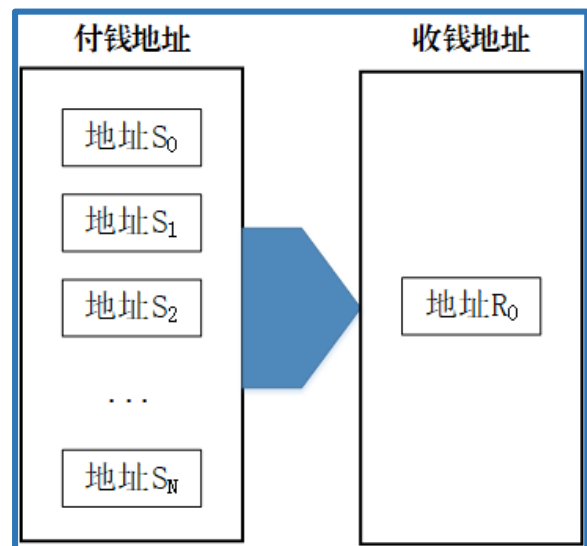
- 区块链——所有信息是公开的
 - YES, 所有“**帐目**”信息是公开的

- 区块链——所有人员是匿名的
 - YES, 所有“**人员**”信息是“匿名”
 - BUT, 所有“**地址**”信息是公开的

- 区块链隐私
 - 身份隐私
 - 交易隐私
- 区块链公开的信息
 - 同一地址的 **身份同一性** 无法掩盖
 - 不同地址之间的 **关联交易** 无法掩盖
 - 不同地址之间的 **特殊交易** 无法掩盖



几种交易方式







Donate to WikiLeaks

WikiLeaks is entirely supported by the general public.

Your donations pay for WikiLeaks projects, staff, servers and protective infrastructure.

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be exchanged for fiat currency faster alternative to other donation methods. You can send BTC to the following address:

36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo  

Various sites offer a service to exchange other currency to/from Bitcoins. Bitcoins are not subject to central regulations and are not legal tender.

安全应对措施 (1)

限制阅
读权限

去链

混币

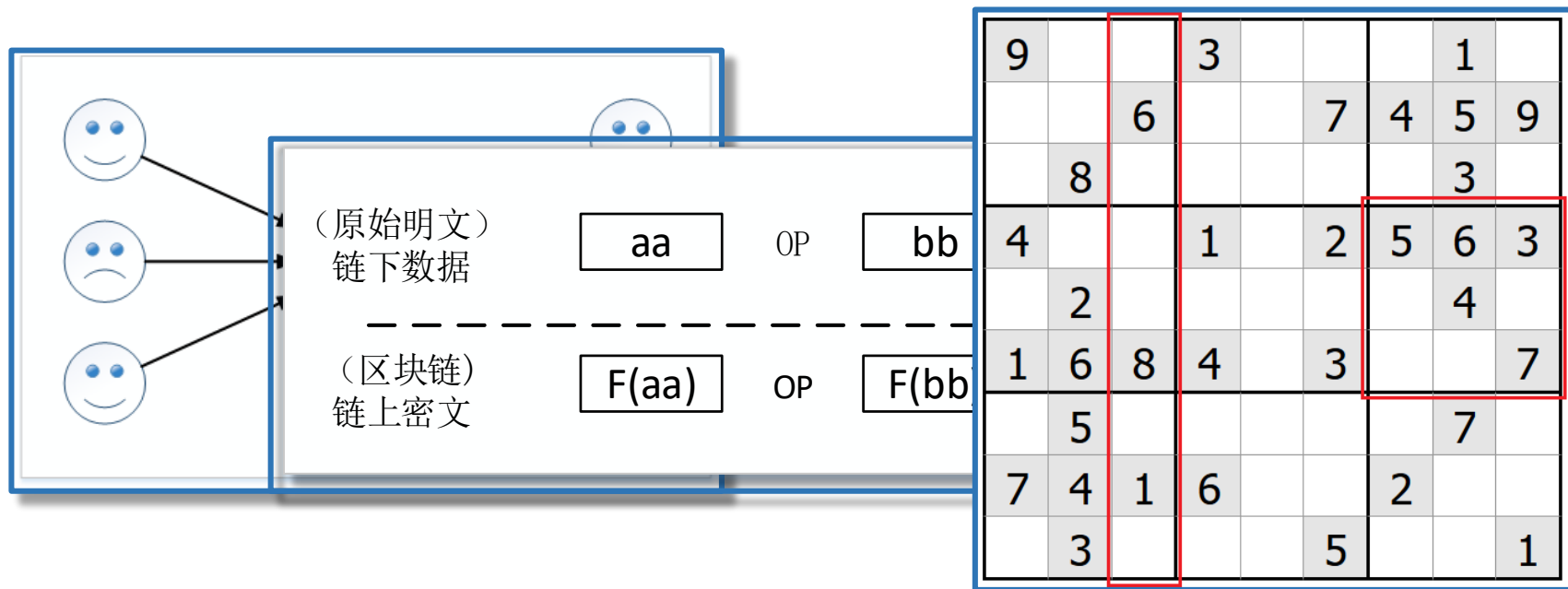
环签名

同态
加密

零知识
证明

安全应对措施 (2)

■ 混币/同态加密/零知识证明



启明星辰信息技术集团股份有限公司成立于1996年，由留美博士严望佳女士创建，是国内极具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。

多年来，启明星辰保持了我国入侵检测/入侵防御、统一威胁管理、安全管理平台、运维安全审计、数据审计与防护市场占有率第一位，针对客户业务推出的整体安全解决方案及安全专业服务可帮助客户建立起完善的安全保障体系。



2018

感谢大家的聆听

Thank you very much & best regards.

