

# 数字货币交易所安全漫谈

北京长亭科技有限公司

杨坤

[kun.yang@chaitin.com](mailto:kun.yang@chaitin.com)

## □ 安全服务

- 渗透测试
- 红蓝对抗
- 应急响应
- 基线检查

## □ 安全产品

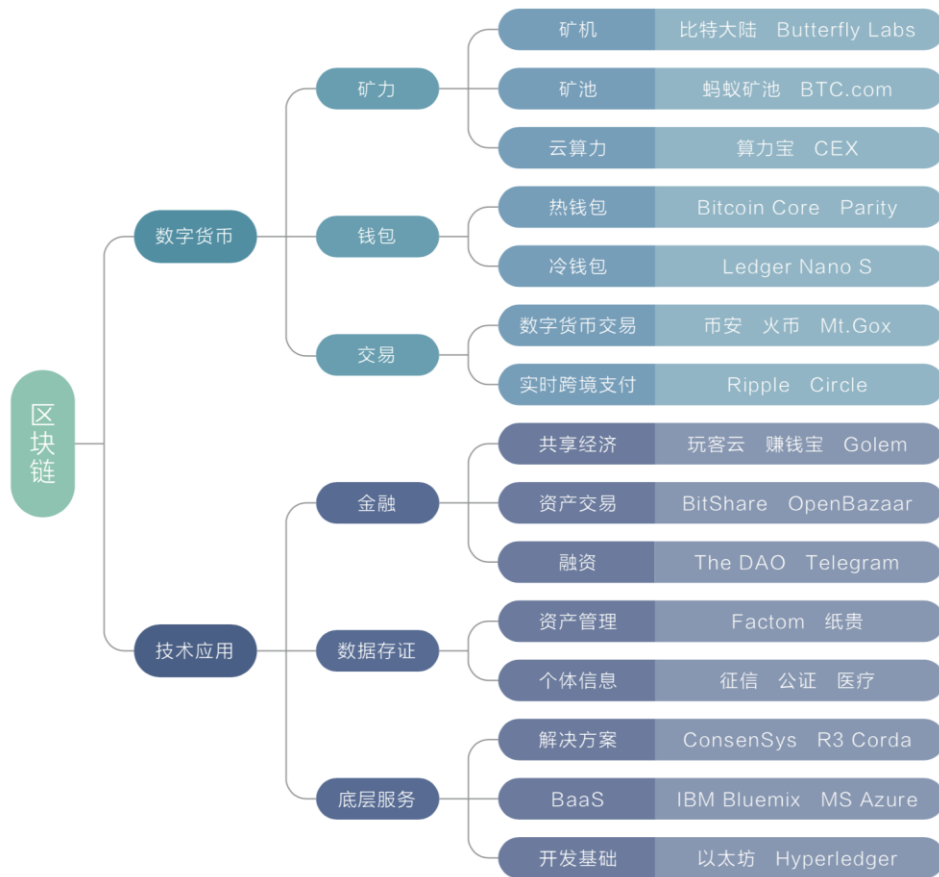
- 雷池Web应用防火墙
- 谛听内网威胁感知系统
- 洞鉴安全评估系统
- 牧云服务器安全平台

## □ 区块链安全方案

- 应用安全解决方案
- 安全研究与事件追踪
  - 《区块链安全生存指南》
- 行业定制化安全服务
- 智能合约审计
- 共识机制安全咨询



- ❑ 行业划分摘自《区块链安全生存指南》
- ❑ 数字货币交易所是区块链行业历史最久、商业运作最成功的行业形态之一，间接推动了区块链应用的发展
- ❑ 另一方面，交易所聚集的资产也吸引了地下黑色产业链的目光



# 细数那些逝去的比特币交易所

- ❑ 《36 bitcoin exchanges that are no longer with us
  - by Brave New Coin
  - 2015年10月23日
- ❑ 2家被收购，继续存活
- ❑ 16家资金困难，2家失去银行合作关系，4家违法
- ❑ 13家遭遇黑客攻击 ( >36% )

Bitcoin Market	MtGox	Tradehill	Bitcoin-Central	Bitcoinica	Bitstake
Crypto-Trade	Intersango	FXBTC	Bitcoin Brasil	Bitmarket.eu	Bitfloor
Bitomat	Bitcoin	Vault of Satoshi	Kaptiton	WeExchange	UpBit
CoinEx	Cyptorush	McxNow	Mintpal	SwissCEX	Prelude
Libertybit	Comkort	AllCrypto	Coin-Swap	Melotic	BitYes
Yacuna	Virtex	Excoin	Bitspark	Coin.MX	Harborly

# “未知攻，焉知防” 交易所攻击案例回顾





- ❑ 2013年，620 BTC被窃取，攻击者通过 **SQL注入** 获得了交易所服务器权限，并转走了资金
- ❑ 微软安全研究人员发现攻击者ID是chinabig01，攻击来源IP来源莫斯科，攻击者并没有使用任何代理进行身份隐藏
- ❑ chinabig01也和Dropbox、Formspring、LinkedIn的攻击事件有关
- ❑ 2016年10月5日，捷克警方与FBI联合捉捕了chinabig01，真名Nikulin



- ❑ 2011年6月，攻击者入侵了Mt.Gox某审计人员所使用的一台电脑，进一步获取包含60,000用户账号的数据库文件
- ❑ 攻击者破解了其中一个大额账户的密码，通过此账户发出大量售卖消息，出售其账下400,000 BTC，试图通过合法交易流程转移资金。
- ❑ 安全措施：限制每天最多转出价值\$1,000 BTC，所以没有给此账户造成太大损失
- ❑ 大量的BTC出售请求使得交易所BTC价格下跌至1美分，导致约\$8,750,000资产受到影响
- ❑ Mt.Gox服务器没有被攻破



# Mt.Gox 盗币事件 2011-2014

- ❑ 2011年，Mt.Gox密钥文件wallet.dat被窃取，当时BTC客户端还未实现私钥加密功能
- ❑ 2011-2014年间，共计850,000 BTC被多次转出，Mt.Gox 很长时间没有发现，最终被迫关闭
- ❑ 某黑客入侵了Mt.Gox CEO Mark Karpeles的博客，并公布了一系列数据，宣称CEO欺骗了用户和投资者
- ❑ Securelist的安全研究人员发现了伪装成Mt.Gox交易管理软件的同类木马Trojan.Coinstealer 的使用痕迹
- ❑ 2017年7月，BTC-e创始人Alexander Vinnik ( ID为WME ) 在希腊被捕





# Bitcoinica 托管服务商被攻击

- ❑ 2012年3月1日，Bitcoinica在Linode上托管的热钱包中超过43,000被盗
- ❑ Bitcoinica表示攻击者很可能掌握了所有托管在平台上的比特币账户密钥，警告所有用户立刻停止向任何旧账户地址转账
- ❑ 2013年4月，Linode再次被攻击，人们猜测本次利用的漏洞可能和2012年这次一样。这次攻击中Linode的域名注册商name.com存在1day漏洞，使得攻击者能够通过中间人攻击截获管理员凭证；Linode本身使用的ColdFusion存在0day漏洞，可以使攻击者直接获得Linode服务器权限



# Bitcoinica创始人被社工

- ❑ 2012年3月1日，Bitcoinica发表声明18,547 BTC被盗
- ❑ 攻击者攻破了Bitcoinica某团队成员邮箱，并伪装成该员工给创始人Zhou Tong发邮件，询问云服务平Rackspace用户名并申请重置密码
- ❑ 平台要求用户和员工不要使用别处相同的密码



# 比特币NXT币被盗

- ❑ 2014年8月，交易所比特币某账户被先后转出51,670,000NXT到攻击者账户，价值超过1000万人民币
- ❑ 比特币与攻击者就在NXT区块上进行了长达数天的公开谈判。最终，比特币付出440 BTC，赎回42,000,000 NXT
- ❑ 比特币官微称，攻击者未能直接攻破服务器，但通过搜索比特币CEO韩林在六七年前留在网络上的信息，分析出了事发前使用的一个密码，从而进入系统盗取比特币
- ❑ 另外，由于当时的PoS铸币机制限制，使得NXT用户铸币时要求钱包时刻联网，因此冷钱包未能起到保护作用，导致直接被攻击者转账

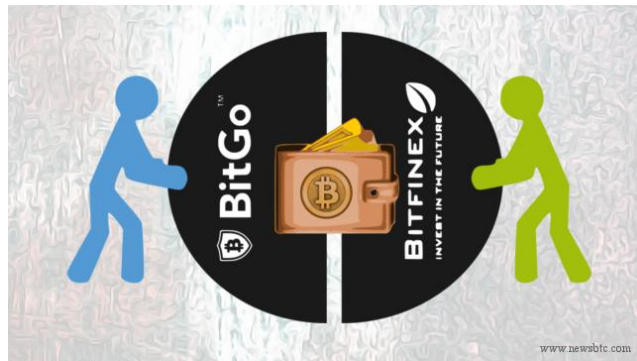
Transaction 5930851748280200080	
Type	Ordinary Payment
Date	Fri Aug 15 2014 14:11:58 GMT+0800 (中国标准时间)
From	NXT-LSC3-VB9T-2W3V-BH7FB
To	NXT-8WJ7-8A2H-MBYN-3W9K4
Amount	51'000'000 NXT
Fee	51'000 NXT
Confirmations	178
Deadline	1440
Block	11441067699374044604

- ❑ 2016年3月，交易所ShapeShift某员工从公司热钱包中盗走了315 BTC，ShapeShift报警并对该名员工提出了民事诉讼
- ❑ 2016年4月7日，在网站迁移过程中，ShapeShift发现其3个钱包又被盗，ShapeShift立即关闭相关服务，重置了所有密码密钥
- ❑ 2016年4月16日，ShapeShift发现热钱包中又被盗57 BTC和2200 ETH。
- ❑ 2016年4月18日，ShapeShift发表声明称，通过调查，发现第一次攻击是在职员工监守自盗，后两次攻击是由于ShapeShift前员工将实施攻击所必需的敏感信息贩卖给了攻击者，三次攻击共计损失\$230,000



# Bitfinex + BitGo多重签名攻击

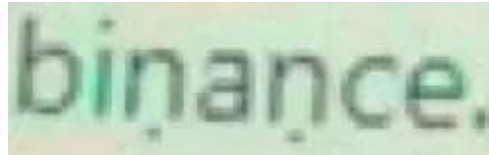
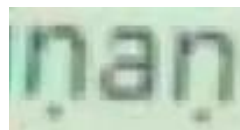
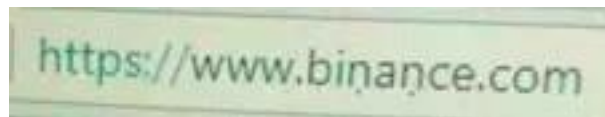
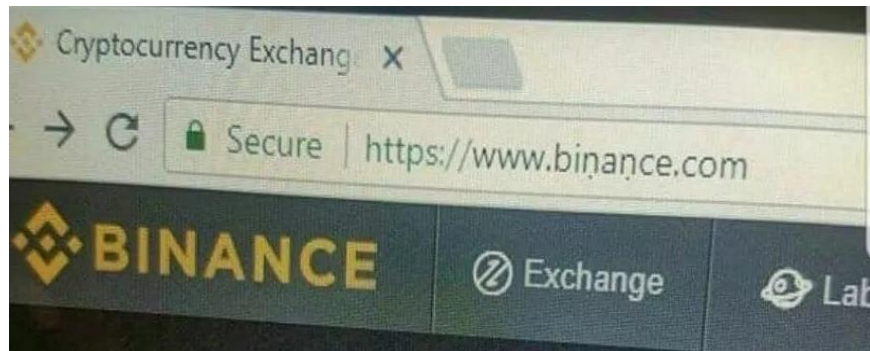
- ❑ 2015年开始，Bitfinex交易所和BitGo合作，共同发布了多重签名钱包系统来管理风险。每一笔交易必须至少使用3个密钥中的2个进行签名认证，Bitfinex持有其中的2个密钥，BitGo持有另一个密钥
- ❑ 攻击者通过某种方式控制Bitfinex的其中一个密钥，并用它对伪造的转账交易进行签名，之后便将交易请求发送给BitGo。BitGo虽持有另一个密钥，但未做身份校验就盲目签名





# 币安钓鱼事件

- ❑ 制作钓鱼网站，积累帐号
- ❑ 通过钓鱼页面骗过二次验证，获取API Key
- ❑ 2018年3月7日，黑客通过大量交易，操纵BTC/VIA市场，在场外间接获利



à á â ã ä å æ ç è é  
ê ë ì í î ï ð ñ ò ó  
ô õ ö ø ù ú û ü ý þ  
š Ÿ œ

- ❑ 应用层SQL注入漏洞
- ❑ 员工个人电脑被入侵
- ❑ 私钥被窃取
- ❑ 基础服务供应商被入侵
- ❑ 运维人员邮箱帐号被窃取
- ❑ 创始人被社工
- ❑ 内部员工攻击
- ❑ 第三方合作商漏洞
- ❑ 平台用户被钓鱼
- ❑ 操纵市场间接获利



# 交易所攻击面分析



## □ 平台应用

- 网站
- 移动App
- API接口

## □ 平台基础设施

- 底层服务供应商（虚拟主机、域名、CDN）
- 主机
- 网络设备
- 内网平台

## □ 核心数据

- 帐号库
- 钱包私钥

## □ 业务逻辑

- 活动
- 风险控制策略

## □ 平台用户


- 帐号
- API Key
- 安全意识

## □ 员工与高管

- 电脑/移动终端
- 帐号
- 安全意识

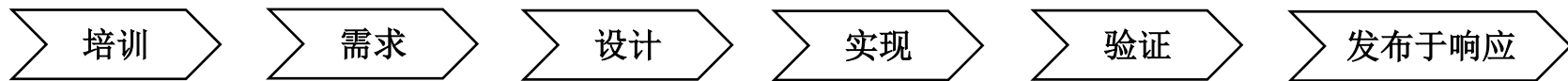
- ❑ 运维缺陷
- ❑ 应用漏洞
  - OWASP Top 10
- ❑ 业务逻辑漏洞
- ❑ 通用软件0day/1day
- ❑ 安全意识漏洞（社会工程学）
  - 内鬼
  - 钓鱼
  - 撞库





# “如何进行系统性防御？” 安全开发生命周期 SDL

# 安全开发生命周期 (SDL)





❑ 大多数的安全问题都是在项目开发过程中由人导致的

❑ 培训内容

- 安全意识教育
- 威胁建模方法与安全设计原则
- 相关编程语言与框架的安全开发
- 智能合约安全开发与审计
- 渗透测试
- 基线与运维安全
- 应急响应



□ 提出功能需求的同时，也要提安全需求

□ 解决三个问题

- 要达到怎样的安全？
- 可能出现哪些安全漏洞，它们的级别是什么？
- 项目的哪些部分需要进行威胁建模、设计评估或渗透测试？



- ❑ 软件的安全问题很大部分是由于不安全的设计引入的
- ❑ 设计阶段产生的安全缺陷在后期修复成本较高、甚至不可修复
- ❑ 设计阶段的几项重要工作
  - 威胁建模
  - 制定安全规范
  - 设计安全架构





## □ 微软STRIDE方法

- 数据流图 ( DFD )
- 六种安全属性STRIDE：假冒、篡改、否认、信息泄露、拒绝服务、权限提升
- 使用DREAD模型量化威胁等级

## □ 攻击树方法



- ☐ 安全编码规范
- ☐ 第三方软件/产品选型规范
- ☐ 密码学/证书规范
- ☐ 安全基线/配置核查规范
- ☐ 运维规范



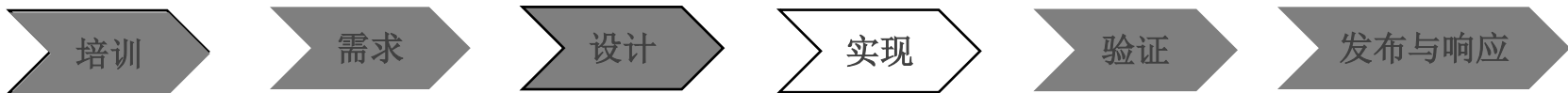
## ❑ 网络拓扑安全架构

- 隔离
- 协议安全

## ❑ 软件与系统安全架构

- 签名、认证、授权
- 密钥管理：存储和使用、定期更换、备份
- 进程隔离
- 权限控制
- 安全存储

## ❑ 业务逻辑安全策略



## □ 根据安全规范和安全架构进行开发

- 统一使用规范的工具进行开发和编译

## □ 代码审计，确保安全规范和设计落地

- 采用静态分析工具对源代码进行扫描
  - 特征比对
  - 程序分析
- 进行人工交互式代码审计

## □ 异常测试，挑战安全架构和策略



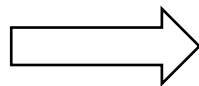
## □ 对完整系统进行渗透测试

- 模拟黑客，使用相同的攻击技术进行尝试
  - 挖掘运维缺陷
  - 挖掘应用漏洞
  - 测试业务逻辑安全
  - 寻找未修复漏洞
  - 测试安全意识
- 白盒审计
  - 请安全专家审计代码





- ❑ 存档发布版本
- ❑ 设立应急响应机制
  - 建立应急响应团队
  - 建设威胁检测能力
    - 流量和日志记录
    - 跟进威胁情报
    - 部署检测设备
  - 制订应急事件处置方案
- ❑ 设立漏洞赏金计划





# 感谢大家的聆听

长亭科技 | ConsenSys | 比特大陆  
联合发布《区块链安全生存指南》

