

比特币交易所安全内幕

火币网 安全总监

周明昊

安全从业者对比特币的印象是...

- 负面印象来自于
- 勒索软件



安全从业者对比特币的印象是...

- 负面印象来自于
- 勒索软件
- 地下黑市



议题内容介绍

比特币行业的
安全案例

分享技术
解决方案

部门间配
合的故事

区块链技
术的未来

作为大蜜罐经历的花式攻击

网站渗透

DDoS
攻击

弱口令
暴力破解

社会工
程学攻
击

针对网
站用户
的欺诈

Mt.Gox的破产



Mt.Gox的破产

什么是Mt.Gox?

- 当时最大的比特币交易平台
- 70%的市场份额
- 75万枚比特币约合4.5亿美元

什么是交易 延展性攻击

合法提币

改变交易的
ID

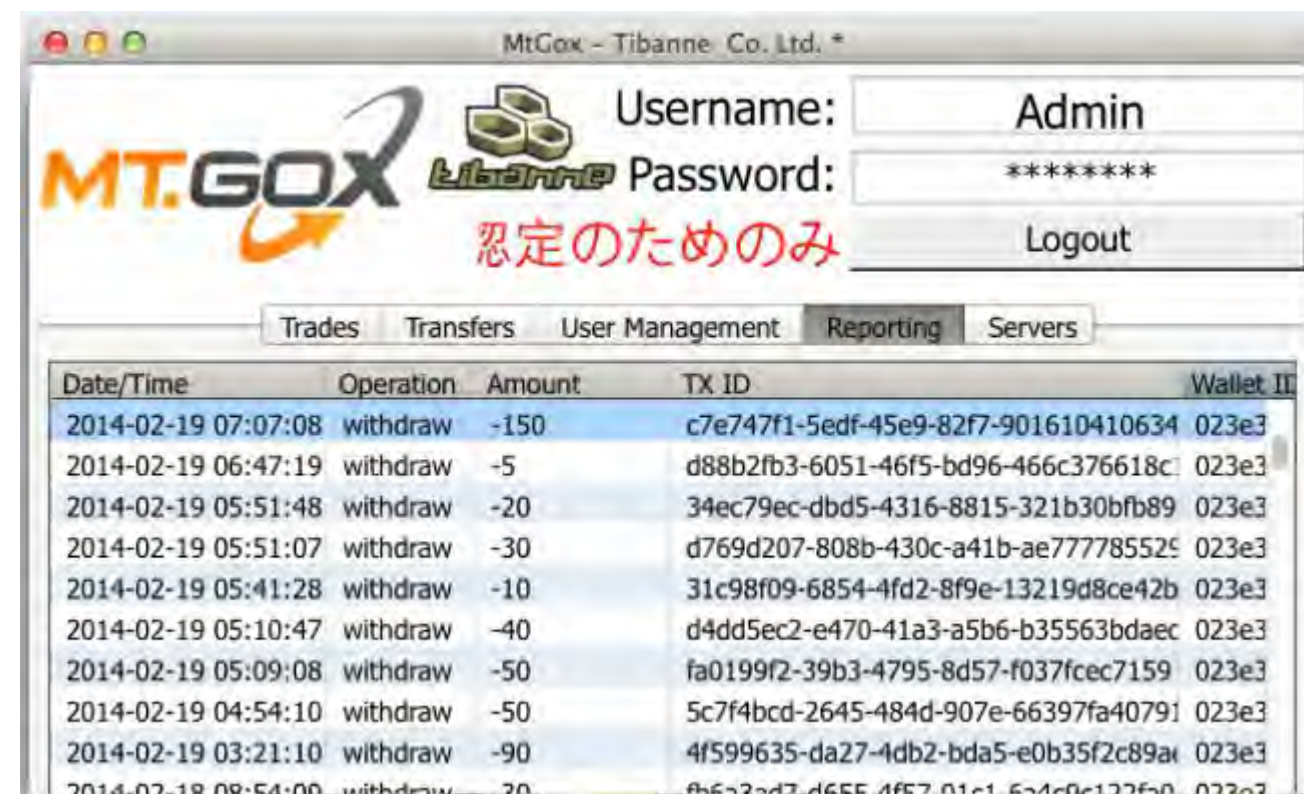
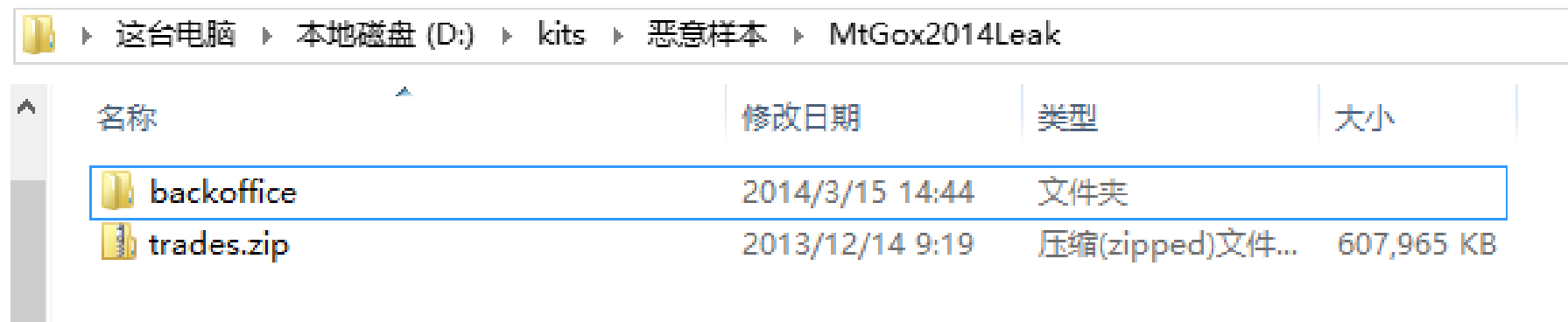
不改变交易
的有效性

申诉没到账

客服补发币

Mt.Gox的倒闭

- 闹剧中还顺带出了一次成功的水坑攻击



Bitstamp的遭遇

- Mt.Gox 70%的用户跑去了Bitstamp和Btc-e
- 系统管理员被社工
- 钱包的私钥被dump，损失1.8万btc

在这之后还发生了许多事。。。。

- 796交易所被盗**1000**btc
- 比特儿被盗**7170**btc
- 比特币存钱罐BTC被盗**3000**btc
- Yes-BTC比特币交易被盗**435**btc
- BTC-e被盗数百btc
- bitfinex热钱包被盗，损失不详
- 最大众筹项目DAO（1.6亿美元）损失超过**6000万美元**的以太币，面临关闭

比特币行业特有的攻击类型

- 交易延展性攻击
 - 用不同的签名方法导致transaction有效，但hash值发生改变
- 一聪攻击
 - 比特币网络的DoS攻击
- DAO攻击
 - 利用智能合约的代码漏洞
- 双花攻击
 - 最终一致性的弱点

Google Authentication的应用

- 超过一半的内网漫游入口为后台弱口令
- 密码验证方式弱口令不可避免
- 后台功能的安全性不可能达到主站的水准



Google Authentication的应用



Google Authentication的应用

- 用户认证使用GA的好处

- 手机验证码的安全缺陷

- 海外用户接收短信稳定性不足

- 保护用户隐私

	绑定邮箱	已绑定	您绑定的邮箱为zho****@gmail.com	
	绑定手机	已绑定	您已绑定手机186****9609	修改
	绑定谷歌验证码	已绑定	经常不能收到短信验证码，建议绑定谷歌验证码。	更换绑定 解除绑定
	登录密码	已设置	登录火币时使用。	重置
	资金密码	已设置	账户资金变动时，需先验证该资金密码	重置

Google Authentication的应用

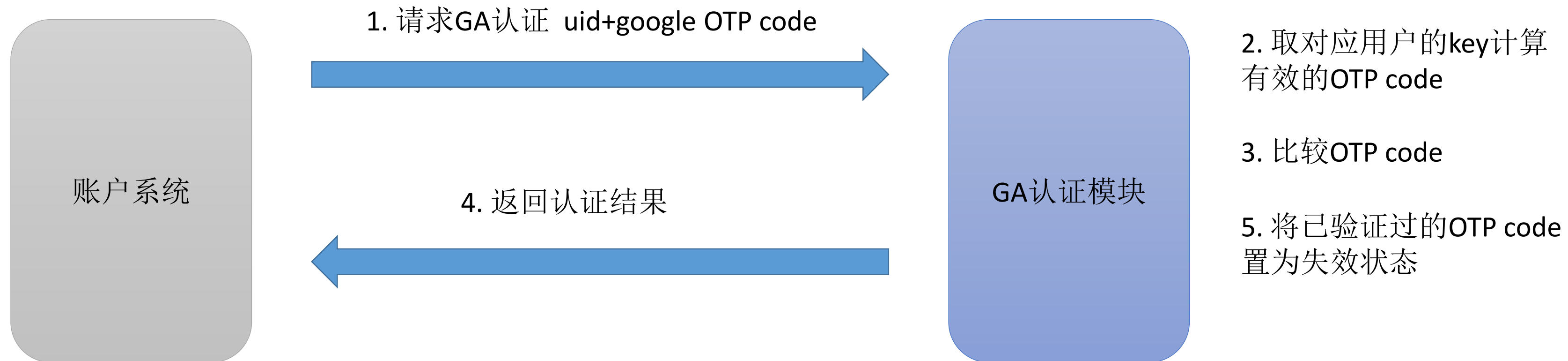
- 好的GA认证模块该如何设计？

User_table	Name	Password_hash		GA_key
1001				
1002				
.....				

NO!

Google Authentication的应用

- 好的GA认证模块该如何设计？



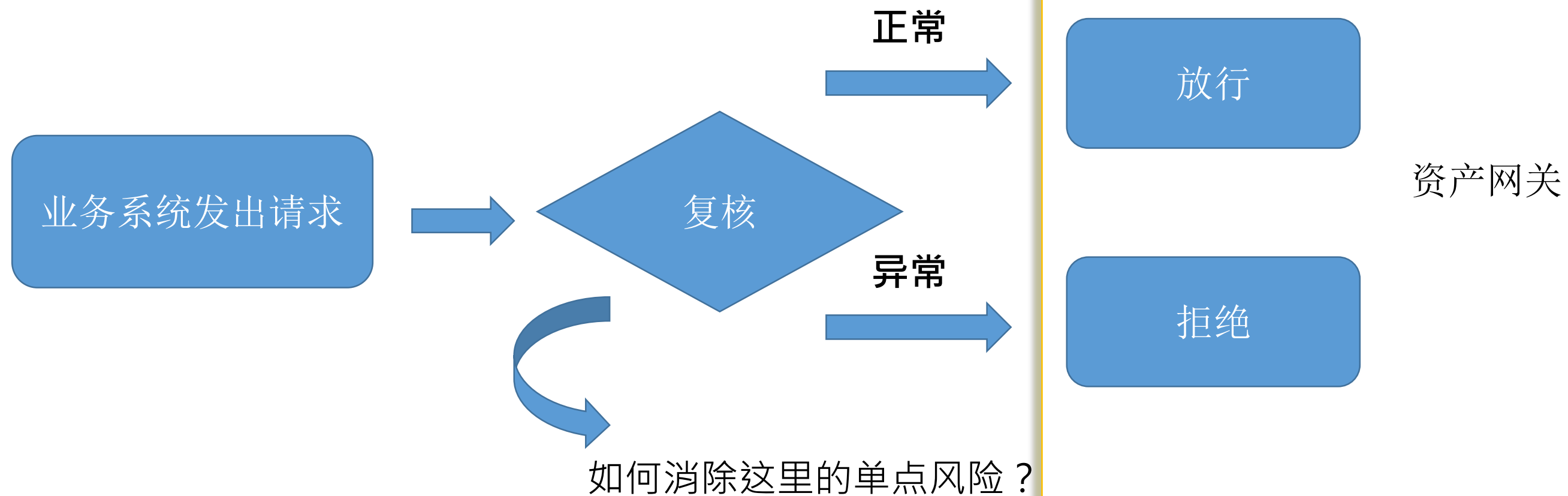
多重签名技术的应用

- 当你要防护一个核心资产系统时.....
- 当发生攻击到造成损失时间跨度很大时
- 安全目标：没有任何一个员工可以获取到私钥
 - 对授权认证方案提出了更高的要求



多重签名技术的应用

- 传统方案的缺陷



多重签名技术的应用

缓解单点风险的代价有多大？

- 分权问题——必须同步操作
- 备角问题——冗余人员多
- 可追溯性差
 - 发现泄漏的原因有 $A+B$, $A'+B$, $A+B'$, $A'+B'$ 四种场景



多重签名技术的应用

- 用多重签名技术来作为资产网关的校验标准

Pay-to-Script-Hash

scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL

scriptSig: ..signatures... <serialized script>

m-of-n multi-signature transaction:

scriptSig: 0 <sig1> ... <script>

script: OP_m <pubKey1> ... OP_n OP_CHECKMULTISIG

至少两个
不同系统
的签名做
授权



资产网关
支持多重
签名的认
证



消除单
点风险

要比产品经理更了解人性

- 安全提币地址的case
- 用户通过严格认证添加安全地址，之后不需要二次验证即可往安全地址提币。
- 这个设计有什么问题？
 - 用户时常不清楚自己行为的后果
 - 至少有10%的有效用户是可以被撞库的
- 工行贵金属诈骗，招行朝朝盈改动

技术团队内部配合如塔防（Tower Defense）游戏

- 核心资产是要守护的目标
- 黑客是源源不断会刷新的入侵者
- 安全团队是防御设计的指挥官



技术团队内部配合如塔防（Tower Defense）游戏

- 运维团队是地形设计师
- 时刻保持最新的“城防图”
- 最怕的是暗度陈仓



技术团队内部配合如塔防（Tower Defense）游戏

- 开发团队是防御塔制造师
- 安全团队要知道会刷什么怪
- 对症下药



区块链技术的优点

- 天然同构系统，数据、协议一致
- 分布式系统显著提升攻击成本
- 数据公开易于校验完整性
- 比特币是第一个成功的实验品，市值¥ 671亿



安全团队招聘

区块链技术促进安全发展的遐想

- 防篡改——可靠的公钥分发渠道，取代CA
- 智能合约——互联网账号遗嘱
- 多重签名——更好的第三方仲裁方式



安全团队招聘

感谢！