

数字资产交易所的安全挑战

汇报人：钟庚发

CHAINUP

当前有多少交易所？



从三大家族到万所大战

 BitForex


 BINANCE

 OKEx

 CoinEx

 CoinBene

 HitBTC

 Huobi

 Bibox

 Bittrex

 B2BX

 BigONE

 Bit-Z

 BitMart

 C2CX


 ChaoEX

 CoinTiger

 DigiFinex

 DragonEX


 FCoin

 Gate.io

 IDAX


 Iquant

 Kucoin


 LBank

 Liqui

 MBAex

 LBank

 OOOBTC

 QBTC

 TOPBTC

 Trade By Trade

据不完全统计交易所丢币超过20亿\$



MT.Gox: 2014-02
比特币失窃, 85万BTC



Bitfinex: 2016-08
比特币钱包, 约12万BTC



Coincheck: 2018-01
约价值5.3亿美元NEM



BitGrail: 2018-02
约1.7亿美元的NANO



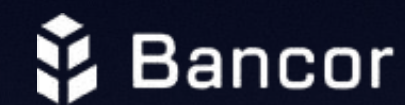
Binance: 2018-03
API-KEY泄露, 操纵币价, 做空



Coincheck: 2018-01
约价值5.3亿美元NEM



SmartMeshToken (SMT): 2018-04
合约漏洞, 1.4亿美元, 及时更换合约



Bancor: 2018-07
Owner私钥遭窃取, 25000ETH



OKEx: 2018-05
USDT转账



Soarcoin (SOAR): 2018-06
合约漏洞, 合约所有者660万美元



Coinrail: 2018-06
黑客入侵, 4000万美元代币



Bithumb: 2018-06
私钥被盗, 350亿韩元

交易所为什么这么不安全？

交易所野蛮生长

法律风险低

攻击即挖矿？

可追溯性差

可直接变现

等等。。。

钱包

- 单一的热钱包
- 不计安全快速上市
- 合约无安全审计

业务系统

- 安全规范
- 风控策略

内控

- 运维体系
- 安全意识
- 权限管制

钱包-合约安全

BEC

```
function batchTransfer(address[] _receivers, uint256 _value) public whenNotPaused returns (bool) {  
    uint cnt = _receivers.length;  
    uint256 amount = uint256(cnt) * _value;  
    require(cnt > 0 && cnt <= 20);  
    require(_value > 0 && balances[msg.sender] >= amount);  
  
    balances[msg.sender] = balances[msg.sender].sub(amount);  
    for (uint i = 0; i < cnt; i++) {  
        balances[_receivers[i]] = balances[_receivers[i]].add(_value);  
        Transfer(msg.sender, _receivers[i], _value);  
    }  
    return true;  
}
```

uint256 amount = uint256(cnt) * _value;

当_value过大，导致amount溢出，变为极小的值

可以通过require(_value > 0 && balances[msg.sender] >= amount);

钱包-快速上市牺牲

很多项目方为了交易所快速接入，提供针对交易所的充值上账，提现出账方法，这些方法多数情况是依赖节点和地址私钥存放在一起，只有这样钱包才能监听到节点的充值，提现；节点的开发性会暴露很多未知的漏洞，从而使攻击者拿到交易所钱包的私钥，包括ETH都曾发生过类似事件

3月20日，安全公司慢雾科技发布警告：有黑客利用以太坊的生态缺陷，使用机器自动窃取网络上的以太坊账户，截至2017年6月10日，已得手207次，账户余额价值约2000万美元。除了以太坊之外，该黑客钱包账号中还有164种其他代币，因为其中许多没有上市交易，价值无法衡量。

攻击者主要是利用转账时候需要unlockAccount账户信息时，不断的发送eth_sendTransaction；keystore存放在节点上 就会出现ETH及代币被盗

钱包-单一热钱包

Coincheck-NEM

正如Cointelegraph在1月26日报道的那样，价值5.34亿美元的XEM被从缺乏多签名安全措施的、低安全性的热钱包中窃取。在Cointelegraph的新闻发布会上，Coincheck的高管们说，所有的资金都存储在一个热钱包或一个在线钱包里，这使得用户的资金容易受到安全漏洞的影响。

很多交易所忽略冷钱包的重要性，以至于事故发生时措手不及

业务-风控策略

- 登录绕过二次验证
- Api-key泄露
- 重要信息修改冻结提现
- 不限制下单价格
- 等等

内部-运维体系

- 私钥泄露
- 误操作
- 随意操作数据库
- 等等

内控-安全意识

- 钓鱼邮件
- 网络没有隔离
- 弱密码
- 等等

内控-权限管制

- 代码仓库
- 服务器细粒度权限管理
- 行为安全审计
- 等等

如何建立风控体系？



钱包

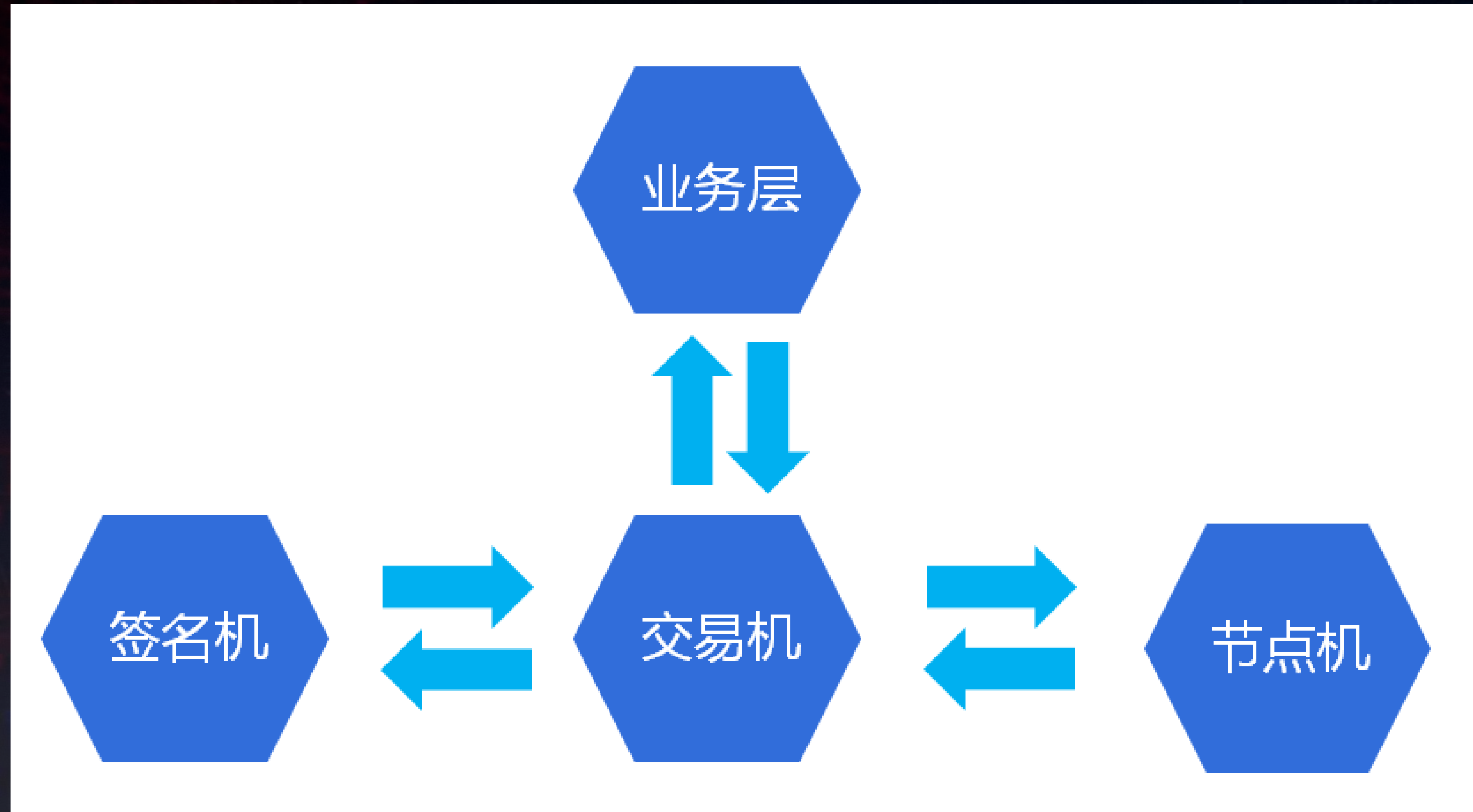


- 合约审计
- 三层结构
- 冷热钱包

钱包-合约审计

- 整数溢出
- 越权访问
- Transfer方法与交易所是否匹配
- 等等

钱包-三层结构



业务



- 充值溯源
- 账户对账
- 提现审核
- 外部扫描

业务-充值溯源

- 钱包自身设计缺陷
- 假充值、双花
- 异常转账信息

业务-账户对账

- 财务流水
- 复式记账
- 个人、公司账户平账

业务-提现审核

- 充值全部真实
- 账能平
- 提现地址正常 - 多用户使用同一个地址提现
- 洗钱行为 - 只充值未交易，或者市价成单迅速提现

业务-外部扫描

- 流入流出
- 私钥被盗
- 系统被黑（比如：非系统地址转帐）
- 充值提现和业务层对比

运维

- 堡垒机
- 安全策略



运维之堡垒机

- 登录日志

操作日期	日志类型	日志内容	用户	来源IP	操作结果
2018-07-27 00:13:01	运维	登录主机: root@47.75.47.22 success	176111405	124.204.17.1	成功
2018-07-27 00:13:01	运维	连接主机: root@47.75.47.22 success	176111405	124.204.17.1	成功
2018-07-27 00:12:45	其他	登录系统	176111405	124.204.17.1	成功
2018-07-26 19:59:57	运维	登录主机: root@47.75.47.22 success	166019695	124.204.17.1	成功

- 操作重放

2018-07-27 02:45:00	字符命令	exit	hk-jump	47.75.47.22	166019695	胡	播放
2018-07-27 02:44:57	字符命令	df -h	hk-jump	47.75.47.22	166019695	胡	播放
2018-07-27 02:44:53	字符命令	fdisk -l	hk-jump	47.75.47.22	166019695	胡	播放
2018-07-27 02:43:49	字符命令	df -h;cat /etc/fstab;mkdir /data/chainup && ln -s /data/chainup /usr/local/	hk-jump	47.75.47.22	166019695	胡	播放

运维的一些安全策略

- 外网隔绝
- 节点机分离
- 内网通讯最小端口权限
- 运维权限最小化
- 签名机单独维护

大数据感知

- 交易模型
- 行为分析
- 指纹
- 链上信息分析



合作共赢



更多合作

THANKES

