# 互联网金融安全实战浅述

付山阳

# 关于我和我的团队

付山阳　　湖南人　爱好篮球和游泳

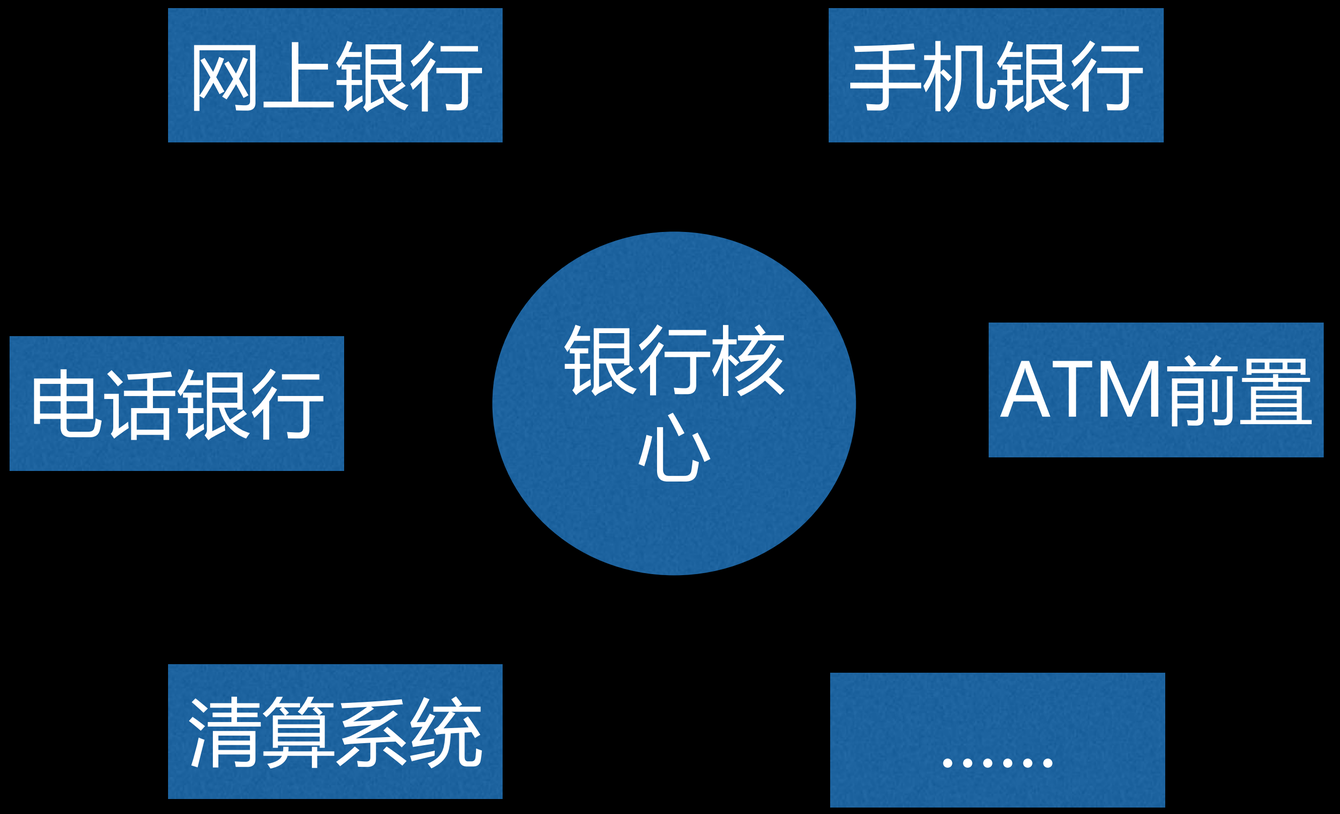
10 years+　安全产品开发和安全运营的工作经验

平安科技产品安全团队负责人（白泽安全团队）

平安银行互联网金融安全负责人

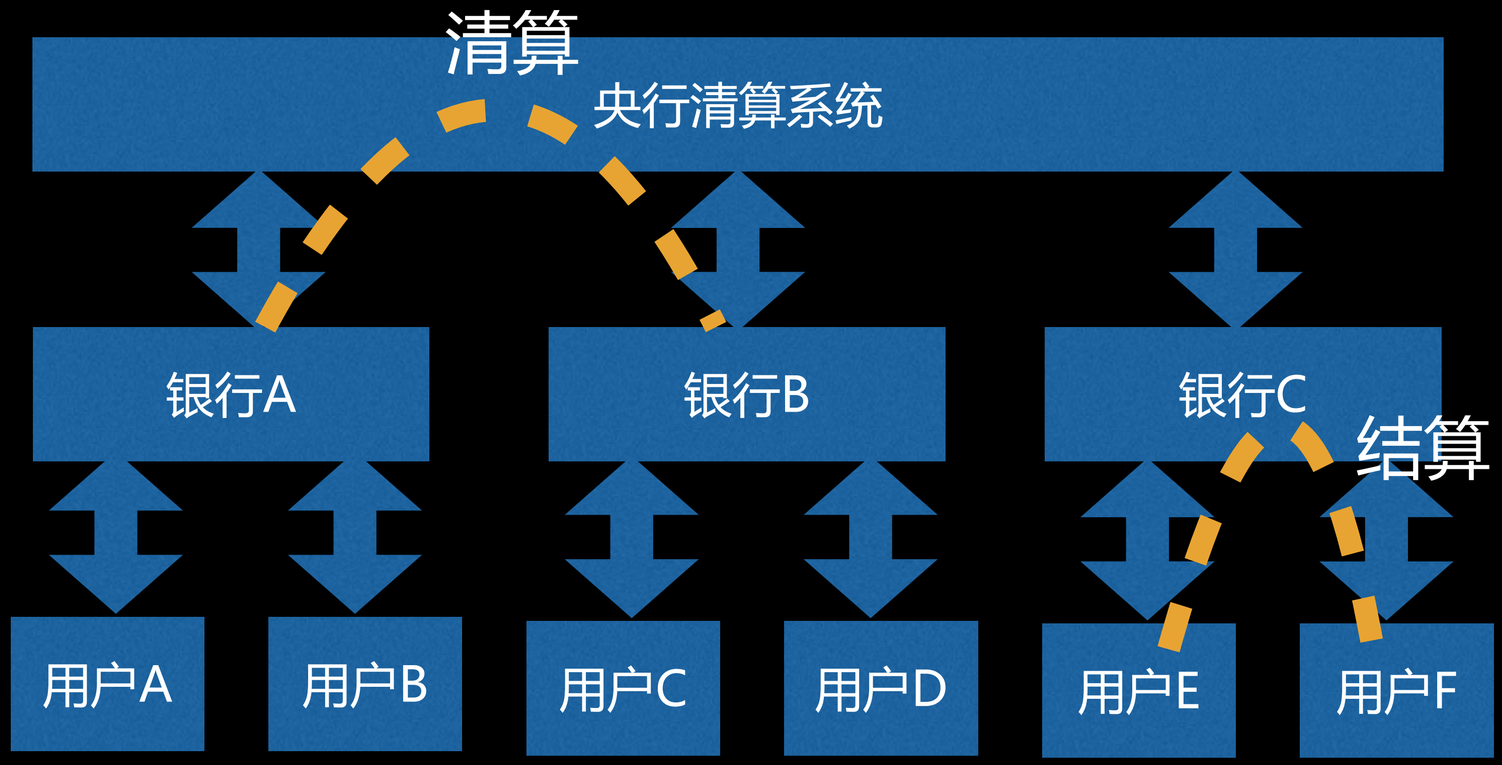
# 目录

# 互联网金融 - 清算系统安全



# 什么是清算系统？

- 通俗地讲，银行与商户、消费者之间为结算关系。
- 而银行与银行之间构成清算关系。



# 史上最大银行抢劫案！

8100万 = 6吨

fandation = 9亿

# 孟加拉银行被攻击全过程

**1、攻击准备**
3个攻击木马
完成编码和
编译

**2、攻击实施**
黎刹商业银行
收到4笔共8100
万美元，并经过
两次转账，进入
3个赌场账户，
其余31笔9亿美
元汇款被暂停

**3、清除痕迹**
修改了其中2
个攻击木马，用
来消除攻击痕迹

**4、发现并追索**
孟加拉国央行
发函要求黎
刹商业银行中
止转账并退款

**5、洗钱成功**
8100万款项
被分5次提取

2月4日
13时45分39秒

2月4日
晚些时候

2月5日
11时46分20秒

2月8日

2月9日

# 孟加拉银行被攻击原因分析

一、**事前**网络隔离，访问控制，权限管理等都很糟糕，密码复杂策略等等都没有。

二、**事中**措施不到位，没有基于网络和主机的入侵检测安全系统，没有有效的对账系统。

三、**事后**的安全应急响应方案没有，或者并不快速和有效的被执行。

# 清算系统的基本IT安全措施建议

**事前**

- 银行跟银行之间应该采用专线传输和双向认证
- SWFIT系统应该部署在单独的服务器上，并且进行网络隔离
- 网络访问应该限制到IP+端口
- 勤快的打补丁
- 定期的安全演习

**事中**

- 要有网络入侵检测和主机入侵检测系统
- 有效的对账系统，区块链能在这块起一定的作用。

**事后**

- 要有成熟快速的应急响应流程，对各种攻击都要有预案。

国内的清算系统安全准备好了吗？

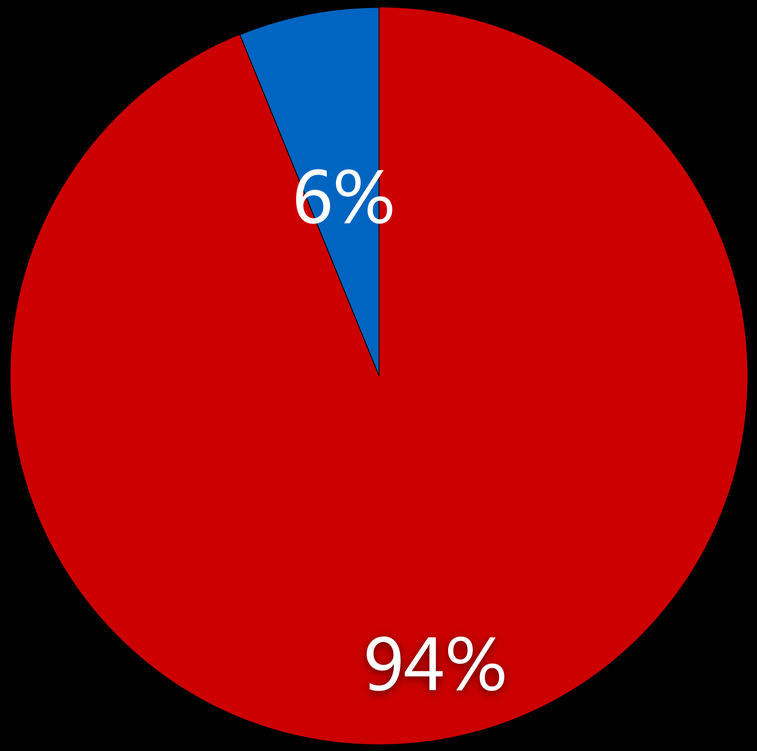
安全应该跟业务同步发展！

# 目录

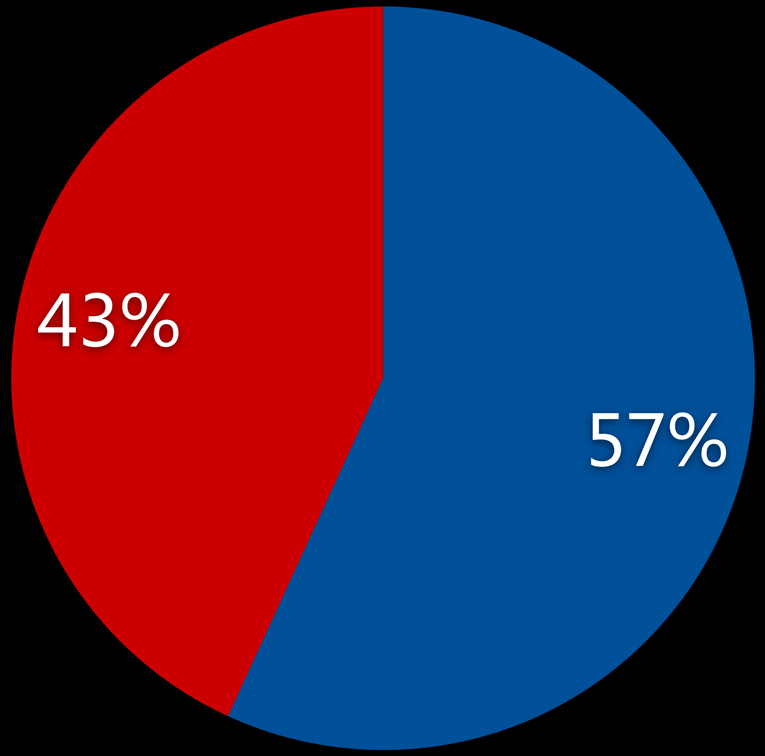
# 互联网金融的移动客户端安全需提升

我们白泽安全团队分析了**146**款互联网金融类APP，其中存在中风险安全漏洞的占比达 **94%**（ **共137** 款APP ），平均每款APP存在漏洞 **11** 个，此外**63** 款APP存在高风险安全漏洞，占比达 **43%**。

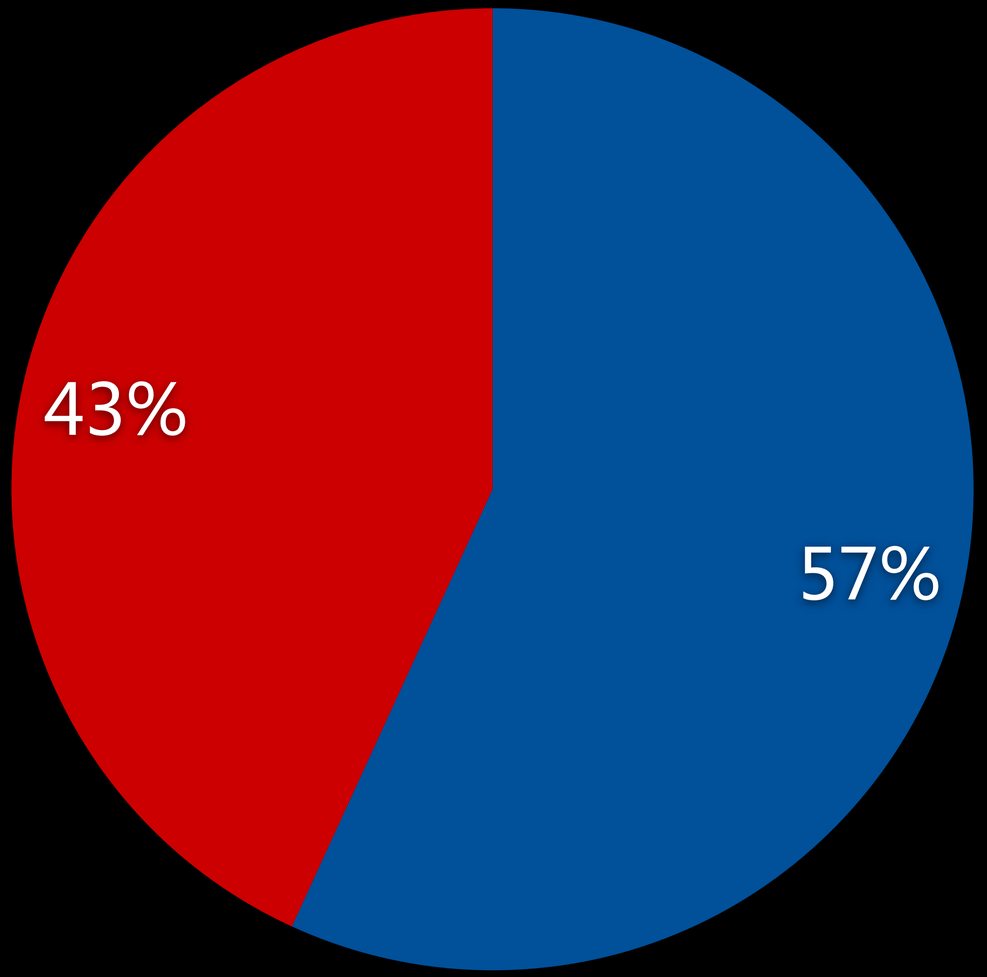
中风险漏洞app占比



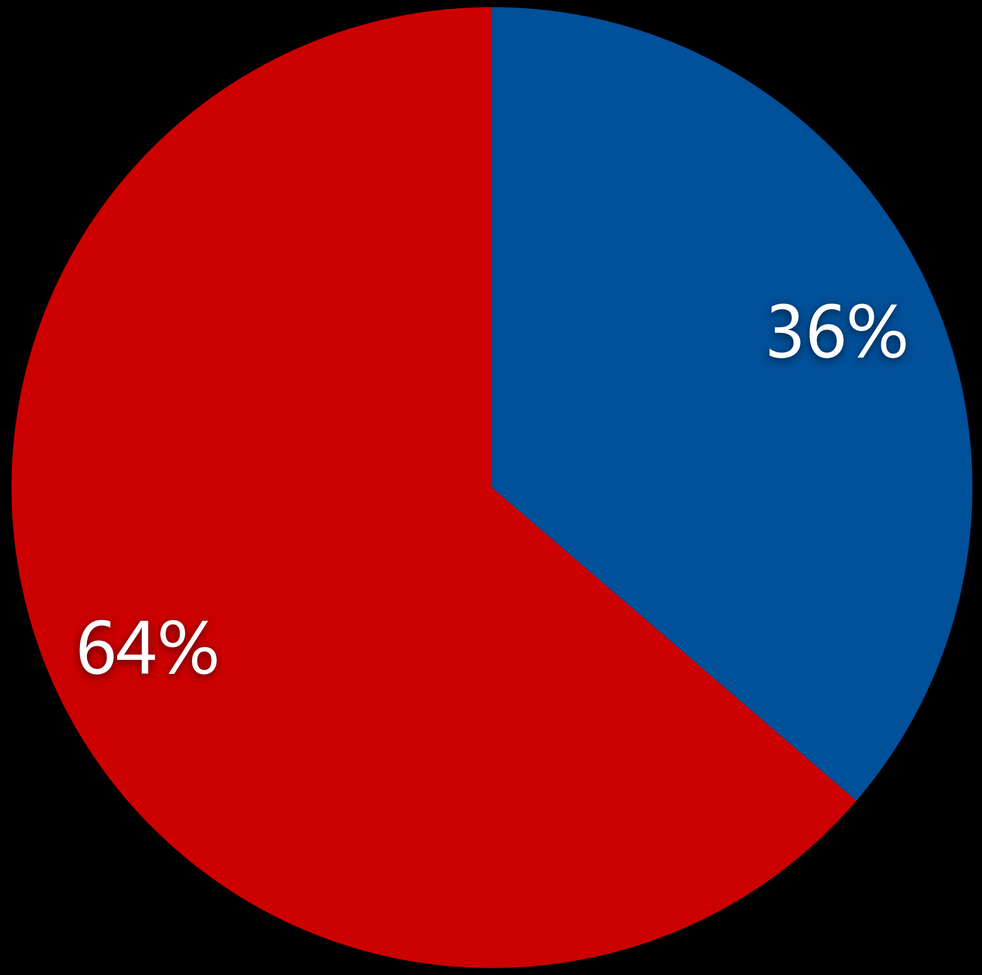

高风险漏洞app占比



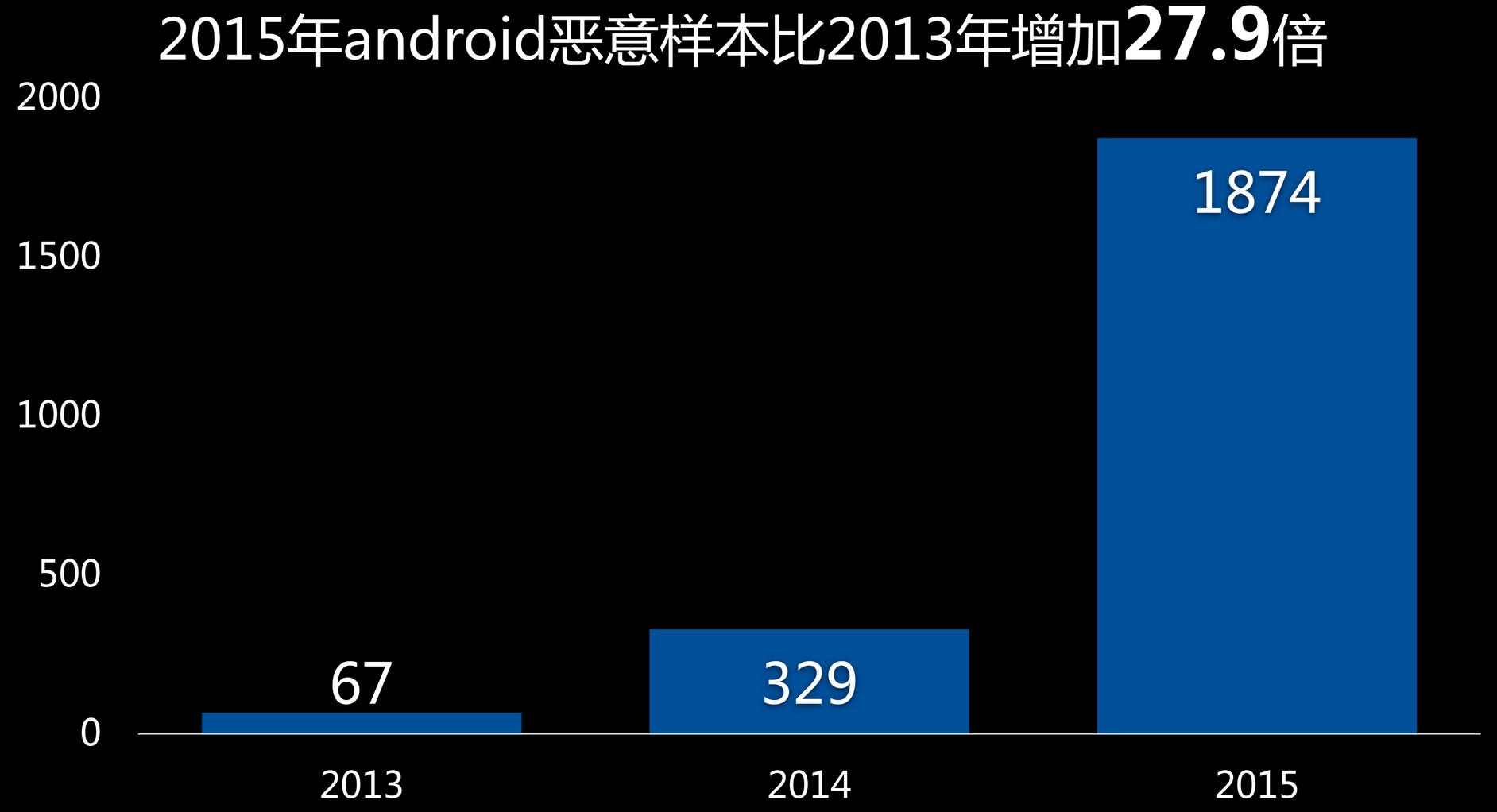
# 四成app存在webview代码注入漏洞



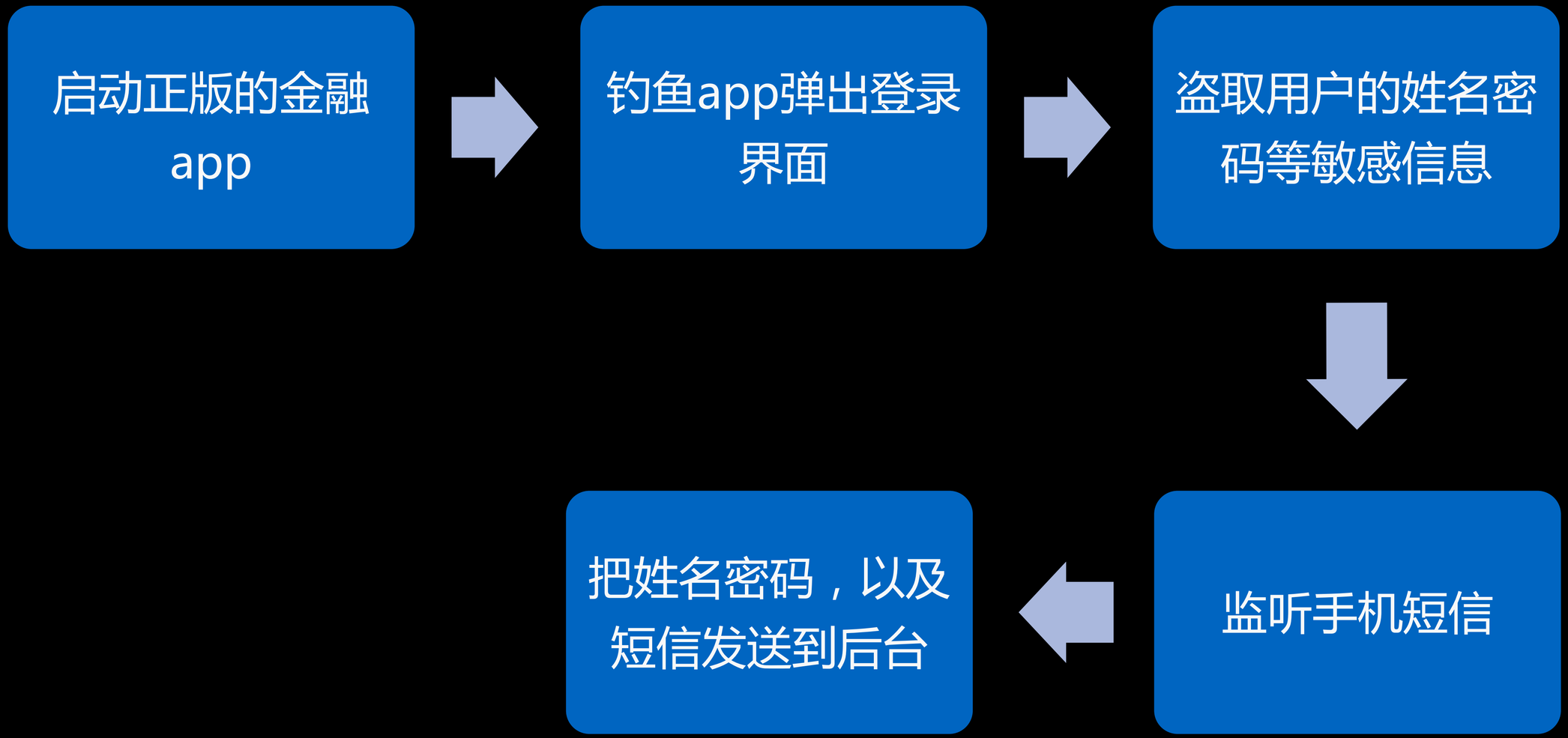
# 六成以上的app未能保障安全传输



# 移动客户端恶意软件问题比较突出



# 互联网金融类android木马的逆向分析



# 互联网金融类android木马的后台调查

# 移动木马攻击的防御建议

**事前**

- 你发给用户所有的短信都不要带链接。
- 提示用户不要点击任何短信链接

**事中**

- 检测是否有activity劫持的情况，并提示用户

**事后**

- 利用用户画像，对钓鱼盗号的登录行为进行判别，阻止盗号者登录。

# 目录

# 互联网金融 - 业务安全

伪冒身份开户

绑卡盗刷

黑中介骗贷

# 伪冒身份开户影响很严重

伪冒身份开户会导致以下两大风险：

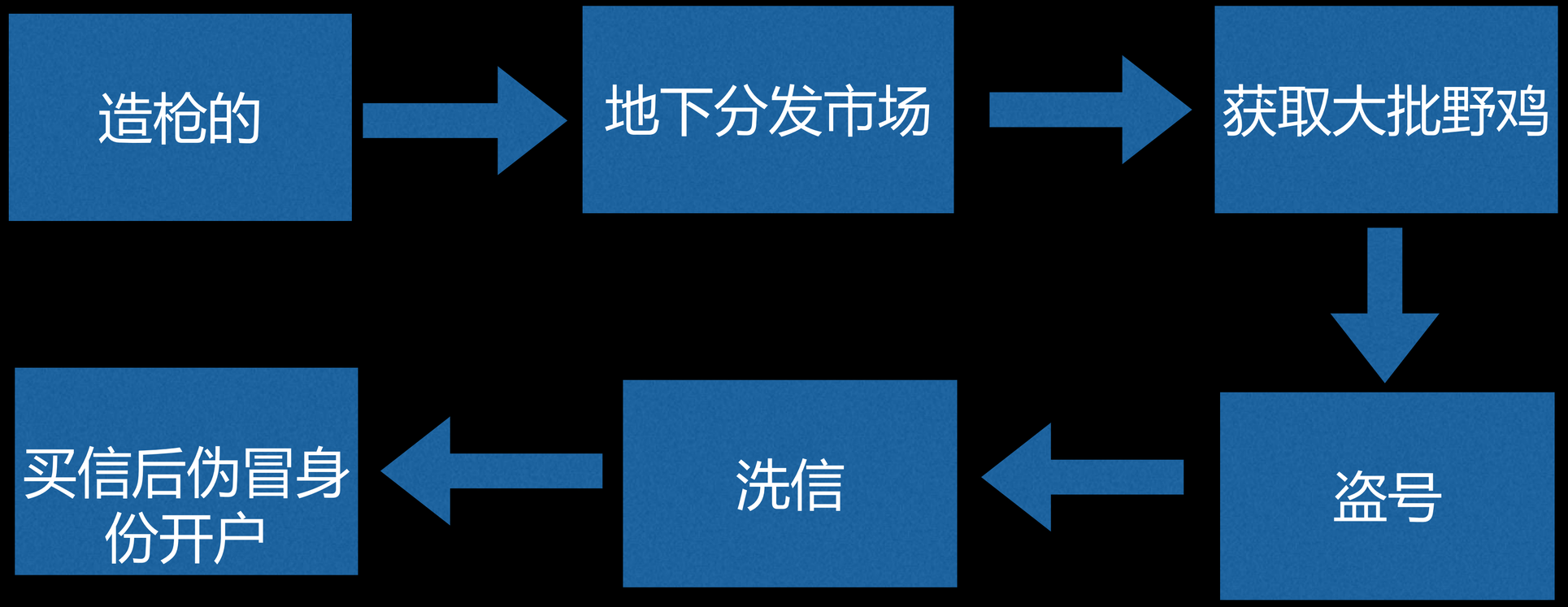
1、洗钱

《中华人民共和国反洗钱法》、《金融机构反洗钱规定》等法律规定金融机构应履行反洗钱义务，否则会被**吊销牌照**。

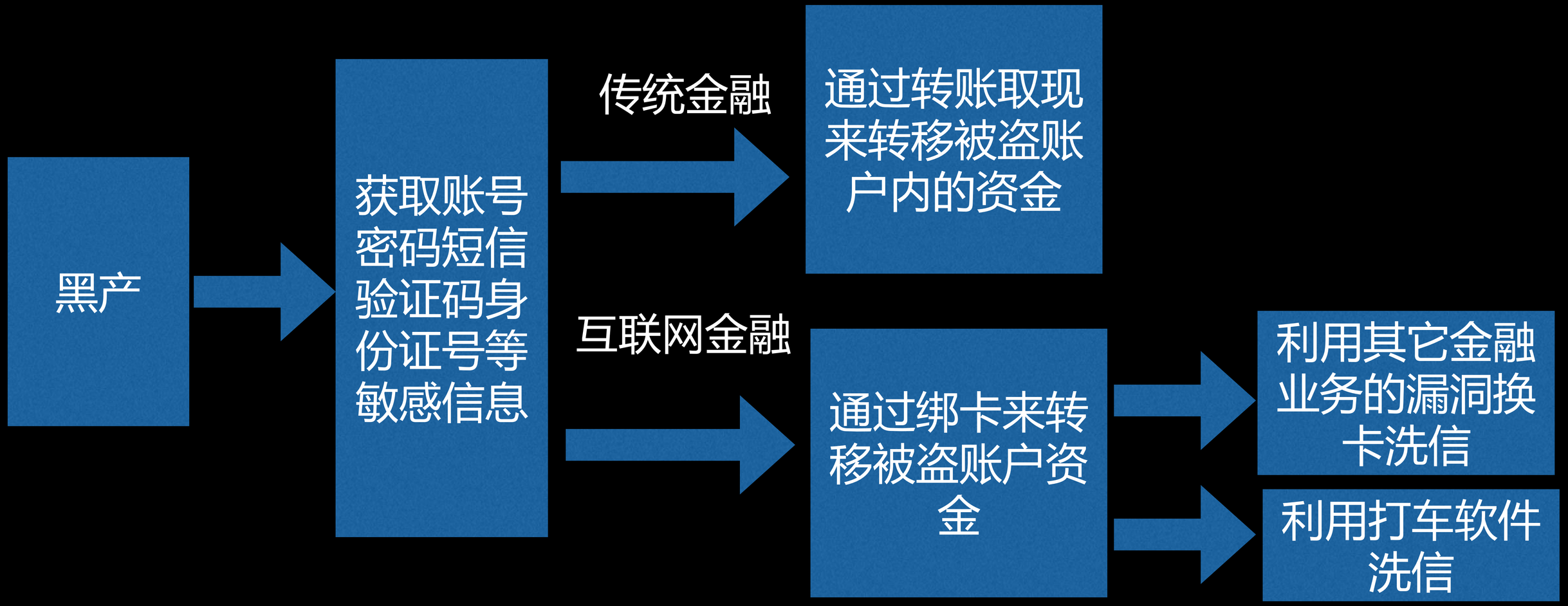
2、骗贷

骗贷会让创业中的互联网金融公司资金损失严重，甚至**直接破产**

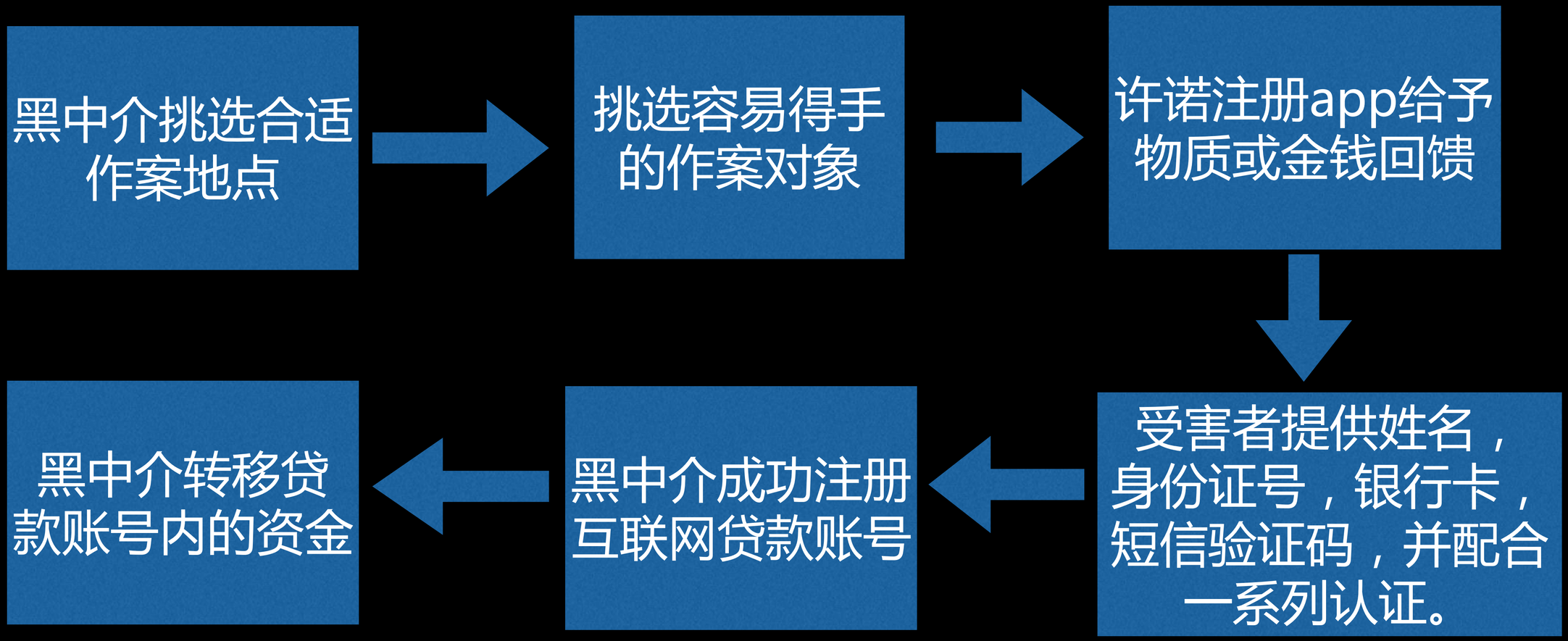
# 伪冒身份开户的产业链分析



# 洗信方式与传统金融时代有所变化



# 传统骗贷的套路也出现在互联网金融上



# 总结

**清算系统安全**

- 分析了孟加拉国央行清算系统的案例，以及这件事件给我在安全建设上的启示。
- 国内的互联网金融安全企业需要注重发展与安全同步进行

**移动客户端安全**

- 互联网金融app有很多的中高风险安全问题，普遍安全投入都不够。
- 移动端的钓鱼问题比较突出，而且有从技术导向转向商业导向的趋势。

**业务安全**

- 分享了三个业务安全的案例，伪冒身份开户导致洗钱，骗贷，影响很严重；洗信的方式与传统金融下有所差异；传统金融的骗贷套路也用到了互联网上。

# Thanks & QA