关于 The Risk Of Payment
创新支付的风险问题

发现

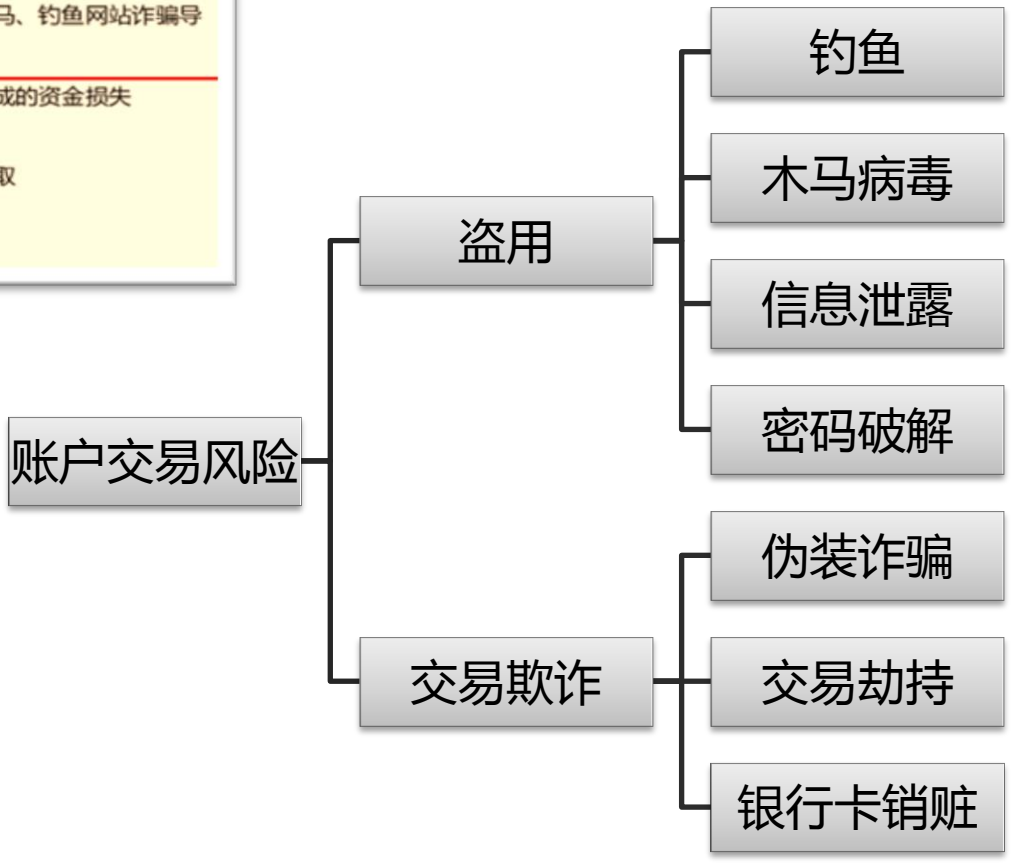
- 创新支付的风险依然是互联网**普遍存在的风险**，比如木马、钓鱼盗号
- 支付创新本质上并**不带来新的风险。**创新集中在接入创新（Ripple和Affirm）和技术创新（识别和数据传输）
- 由于创新的支付特定的应用场景而带来是**风险放大**，比如条码的开放性，容易植入病毒

1

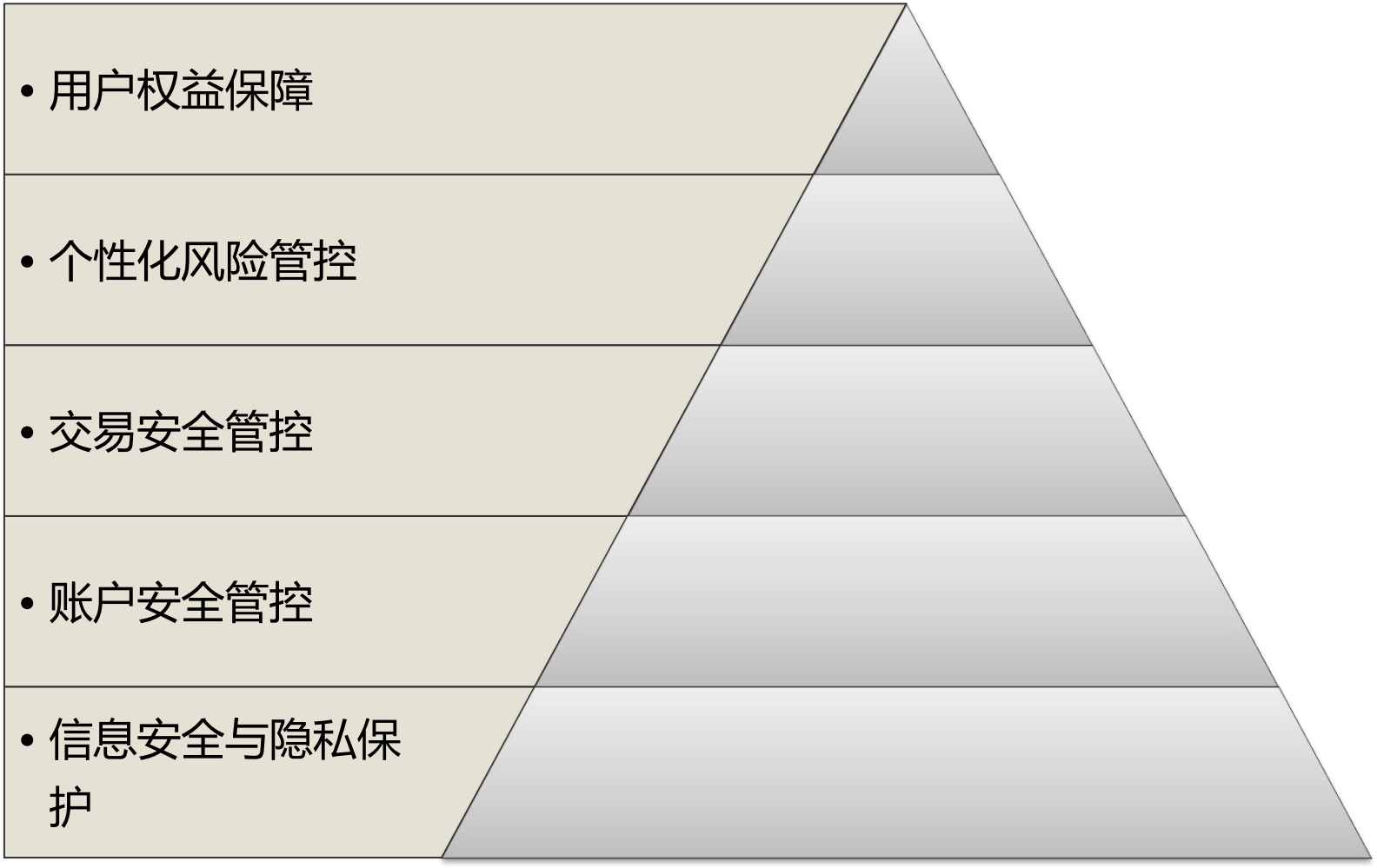
Paypal风控现状

Benchmark

风险挑战：账户交易面临的风险



用户风险管理层级



账户安全管理

客户身份识别

- 实名认证
  - 公安网验证
  - 银行卡验证
- 身份验证保护
  - 密码问题保护
  - 短信确认
  - 图片验证码
  - 加密保存

账户保护

- 安全产品管理
  - 安全控件
  - Ukey
  - 动态口令
  - 数字证书
- 硬件和IP识别
- 二级校验和人工核查
- 黑名单系统

行为安全——行为分析和管理

Defend

- 安全控件
- 数字证书
- 手机动态口令
- 安全教育
- 防钓鱼措施

Adapt

- 用户权限控制
- 交易额度控制
- 风控名单库
- 安全检测
- 增强身份认证

Detect

- 分析引擎
- 安全模型
- 规则维护
- 规则运行分析
- 人机识别

数据安全：客户数据分类和分级管理

客户数据分类

认证信息	隐私信息	交易信息
登录密码 支付密码 密码保护问题答案	动态密码 短信校验码	卡号 有效期 CVV2等
	姓名 身份证号 地址信息	
	手机/电话号码 电子邮箱	
	单笔交易信息 交易统计信息	
		账户余额

分级标准

- 使用范围
- 敏感程度
- 影响范围
- 影响程度

具体定级

- 秘密：
  密码/密钥
  安保问题
  卡信息
- 敏感：
  手机号
  身份证号
  通信地址
- 内部：
  余额
  消费记录
  账务明细

风险管理作业体系

监控体系

- 实时交易监控
- 钓鱼地址识别拦截

投诉与舆情快速反应机制

- 业务投诉处理
- 外部信息收集处理

紧急响应机制

- 应急响应小组
- 应急响应事件标准

账户风险处罚

- 欺诈处罚
- 套现处罚

商户风险处置

- 商户监控
- 警告、整改、清退、禁止续签

风险准备及赔付机制

- 风险准备金账户
- 合理赔付机制

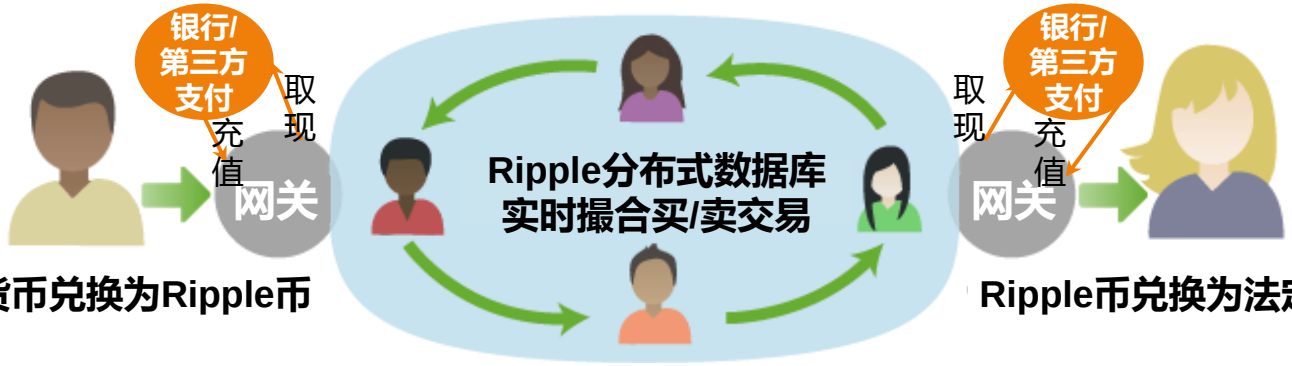
2 业务模式颠覆

Overturn

互联网思维的转账协议

ripple

业务模式



法定、虚拟货币兑换为Ripple币

Ripple币兑换为法定、虚拟货币

Ripple网络

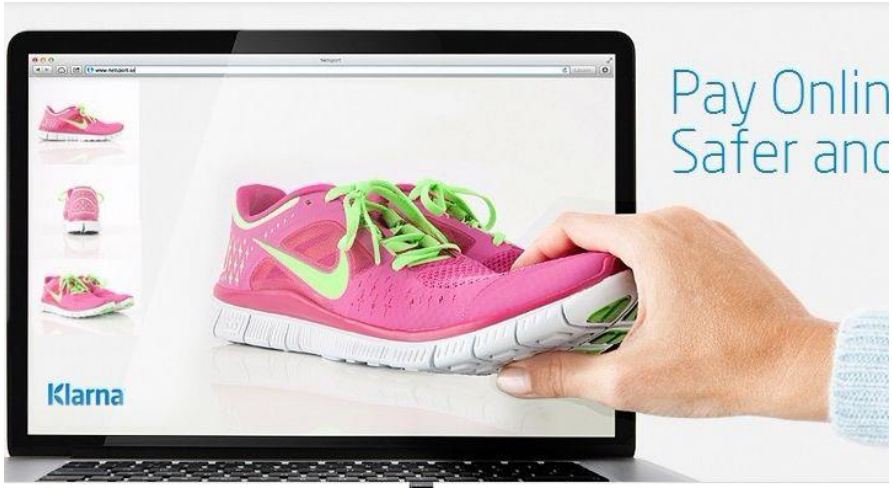
应用

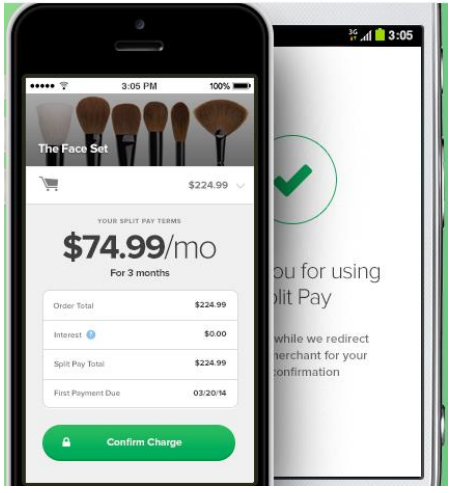
- 不同货币可以随时、免费汇兑、跨境支付
- 不同支付系统间的转账支付，比如壹钱包人民币帐户转渣打银行美元帐户

风险

- 开源项目蕴含技术风险
- 不可信的网关跑路、倒闭造成资金无法结算
- 发行和维护公司opencoin倒闭，会造成ripple币暴跌，从而影响ripple网络

信用来支付





应用：用Facebook账号登录，然后在支持Affirm付款方式的网站上它会帮你先垫付，然后你在30天内付款给Affirm就好

风险：

1. 盗号（钓鱼、木马等）
2. 网络欺诈形成坏账；逾期还款形成呆账

3 技术创新

Innovate

Square

支付流程

风险：

1. 侧录-盗刷：不法分子将一种具有记忆储存功能，可将持卡人的资料以及磁卡的磁条代码全部读出并记录储存下来的设备安装在POS机具上，秘密侧录消费者信用卡信息资料，以便制造“克隆卡”进行盗刷
2. 套现、套扣率
3. 洗钱

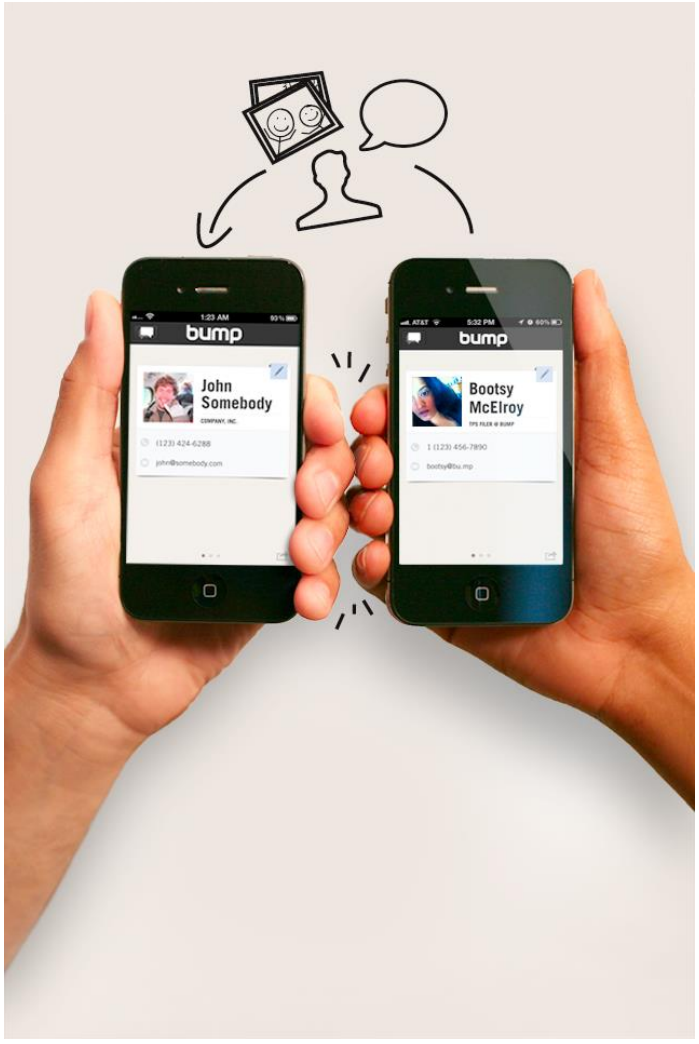
声波

代表：
Zoosh、支付宝、惠尔丰

应用：
利用超声波让手机通过麦克风和扬声器就能完成一次近场通信，两只手机“碰一碰”，支付就完成

风险：
黑客可以使用数据接口远程发起交易并劫持确认刷钱。理论上有风险，但实际支付场景中，即使获得了声波数据，在同一支付场景中也难以对数据的非法利用

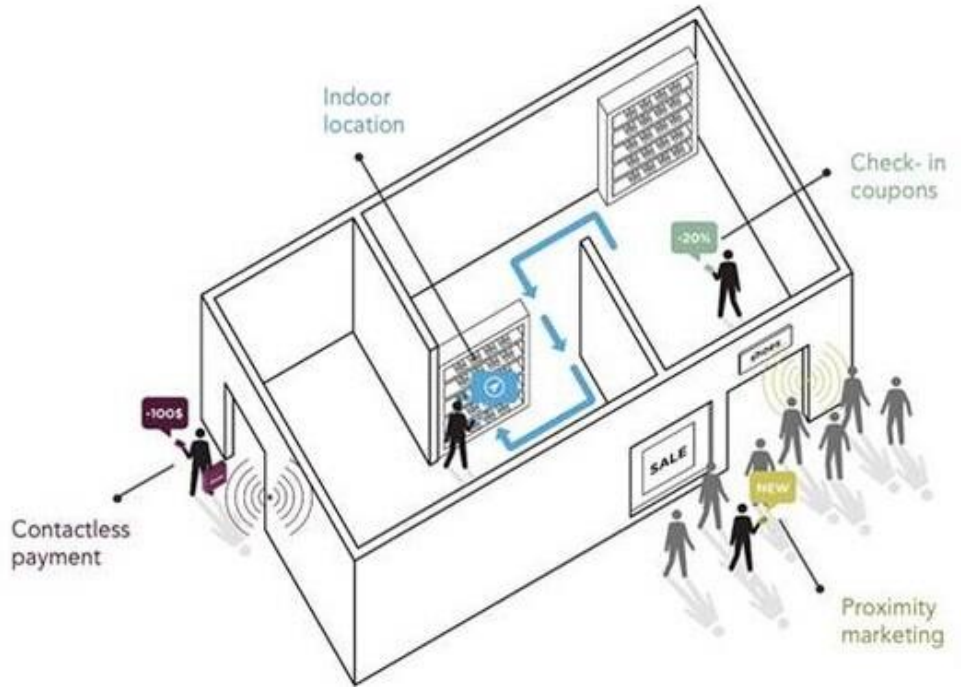
Bump技术



原理：
Bump 的服务器会根据设备间撞击的时间，地理位置，IP 地址等数据来识别身份。通过撞击的时间来判断哪两台设备需要连接

风险：
本身很安全，风险出自接入的非法wifi，容易被窃取用户个人信息和密码

Beacon模式



1. 代表：Square、Paypal、平安
2. 风险：

Ibeacon的格式是公开的，能制作出与正规模块发送相同信息的假冒Beacon模块。不法分子有可能钻商店积分服务的空子，利用假冒模块，发送与积分服务相同的信标，在不用到商店去的情况下无限制地获得来店积分

扫码

被动扫

主动扫

风险：

1. 在条码支付过程中，确认过程简单，黑客可以使用数据接口远程发起交易并劫持程序直接确认刷钱
2. 通过扫描二维码就可以做交易验证，防范意识差的用户见码就扫很容易受骗下载并安装了恶意软件，从而造成资金损失

图像

Jumio™

应用：
它使用摄像头来读取信用卡信息，包括信用卡号码和到期日，接下来输入密码就可以支付

风险：
如果黑客发起收款给劫持后的手机很可能远程操作付款


规避风险，
安全远航