# 区块链安全研究报告

2018 年 8 月

TokenClub 研究院

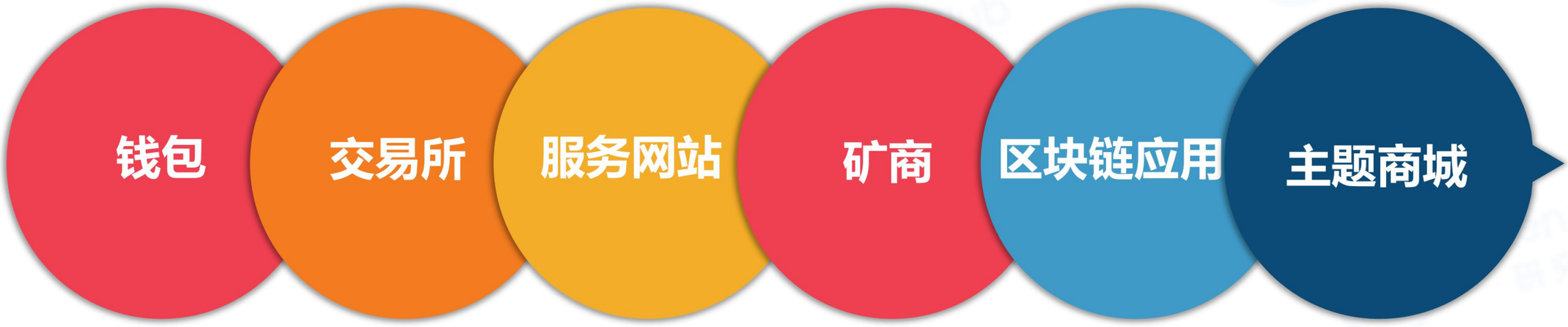
# 目录

# 1.区块链安全行业综述

## 1.1 区块链行业

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算技术的新应用模式。作为比特币的底层技术，它通过时间戳将区块首尾相连形成一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

自比特币诞生以来，区块链行业发展已有近十个年头。在这段过程中，第一家加密货币交易所上线，Paypal、Bitpay 等支付商与比特币厂商建立合作关系，自此加密数字货币顺理成章的融入了整个世界的金融体系中。




随着区块链技术进一步成熟、生态进一步扩大、用户人数以及应用场景进一步发展，各种围绕着数字货币的应用以及基础设施也不断地丰富完善。目前最大的基础设施主要包括以下六类：钱包、交易所、服务性网站以及矿商、区块链应用、数字货币为主题的商城等等。

基础设施的发展与完善相当于为用户开辟了一条更宽阔的路径，更便利的体验能够吸引更多的用户参与到这个市场，更多的用户又能激励更多的服务商提供服务。与此同时，区块链技术本身也在进一步向前推进，2017 年更是借助以太坊在智能合约上的优势带动了整个行业的大爆发。

到目前为止，基于各种应用的参与方式，区块链主要分为公有链、联盟链、私有链。除了我们接触较多的公有链及链上的应用，联盟链与私有链也需要安全技术保驾护航。

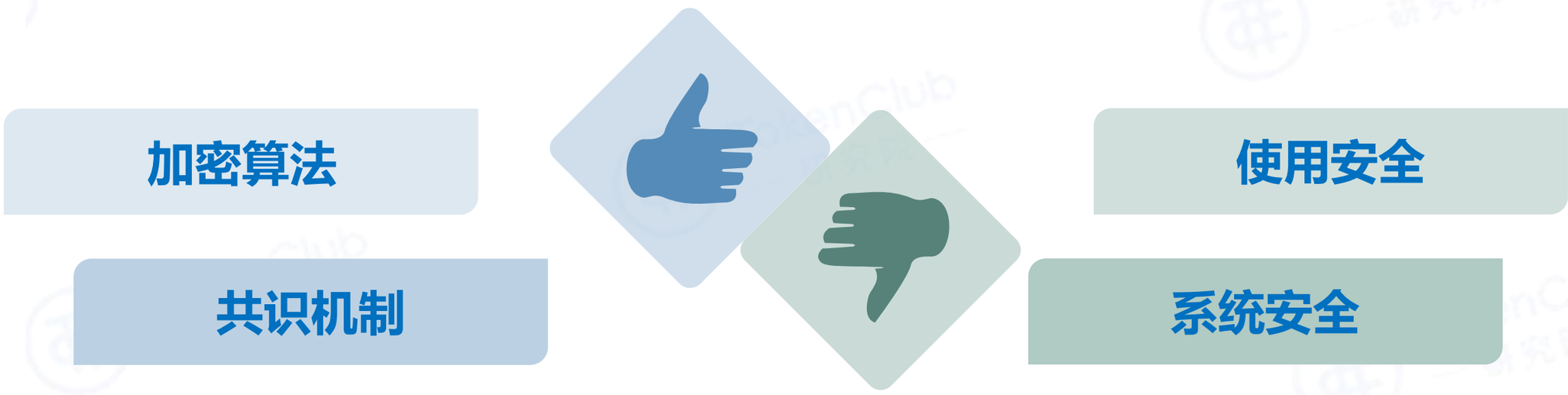

- 公有链：世界上任何个体或者团体都可以发送交易，且交易能够获得区块链的有效确认，任何人都可以参与共识过程。公有链是最早的区块链，也是目前共识最广泛的区块链。是指像比特币区块链这种完全去中心化不受任何机构控制的区块链。

- 联盟链：是指有若干组织或机构共同参与管理的区块链，每个组织或机构控制一个或多个节点，共同记录交易数据，并且只有这些组织和机构能够对联盟链中的数据进行读写和发送交易。

- 私有链：也就是完全私有区块链（Fully private blockchains），是指写入权限完全在一个组织手里的区块链，所有参与到这个区块链中的节点都会被严格控制。

# 1.2 区块链安全性

2018 年 1 月 7 日，整个加密数字货币总市值达到历史最高的 8000 亿美元的市值。基于区块链行业仍处于一个早期阶段，很多安全漏洞尚未被发现以及部分技术人员的安全防护工作并不是很成熟，巨大利益的诱惑下吸引了互联网行业大量的攻击者。




区块链安全吗？通常在描绘比特币特点的时候，人们会将安全性加入其中，这主要是因为比特币的加密算法 SHA256 保证了私钥的难攻破性；另一方面区块链中拥有更多的节点，保证了即便单一节点被攻破，仍然有其他节点保护整个数据库的安全性与完整性。但这两种特点并不能代表区块链安全的全部内容，区块链作为一个庞大的生态，用户作为市场的参与者与投资者，需要对数字货币的买卖与使用。这涉及到从钱包、交易所、私钥保存到共识机制、协议及整个系统的安全性，在这些方面区块链安全问题依然没能得到很好的解决。

随着区块链技术的广泛应用，随之而来的安全问题也愈发增多。由于区块链技术拥有全球性、去中心化、匿名性等一系列特点，目前在资本行业被大量使用，其中用于投资的场景也越来越多。正因为这一系列的特性与场景结合，随之而来的各类攻击也开始不断出现。主要体现在从之前的区块链底层安全技术研究曝光，发展到后来越来越多的虚拟货币被盗，交易所被攻击等事件。而这些只是目前被暴露的一部分，随着区块链技术所产生的价值越来越高，所面临的攻击将持续增加。

频发的安全问题严重影响了行业参与者的数字资产安全，这会影响投资者的信心与体验，行业中的各项基础设施也无法快速稳步的推进；同时对于行业外的人进入到区块链行业也会有很大的影响，从而导致整个行业陷入沉寂。因此，在行业良性发展的同时，针对行业中安全问题频发的板块，通过技术手段做到治理与防范，是这个行业的重中之重。

# 2.行业安全问题

## 2.1 行业安全分类

区块链行业发展到现在，安全事故频频发生，经统计主要集中在以下三个板块：区块链自身机制、区块链生态安全、区块链使用安全。

### 2.1.1 区块链自身机制

由区块链自身机制所引发的安全问题主要体现在三个方面：加密算法的安全性、协议安全性、系统安全性。


密码算法的安全性主要是指基于区块链的公钥算法以及哈希算法，比特币的算法是 SHA256，通过数学难度来保证私钥不被破解。不过随着计算能力的提高以及量子计算机的发展，加密算法存在着被破解的可能性，不过目前来看可能性较低。

协议安全性主要是指该区块链所依托的协议层存在着被攻击的可能性。以比特币为例，矿工通过算力竞争来打包交易记录，当一个节点能够控制全网 51%的算力，那它就有能力推翻原有已确认过的交易，使得恶意双花成为可能。目前各大加密货币算力比较集中，前十大矿池大约占 80%以上的算力，由于大市值加密货币发动算力攻击会对发动者本人造成更大的损失，在博弈论的基础上不太会发生，而小市值低算力保护的币种则会遭受大算力的威胁，比如前段时间遭受算力攻击的 BTG。

系统安全性是指区块链的智能合约在创建以及编写的过程中会存在一些安全漏洞，这些漏洞会给黑客留下攻击的空间。

### 2.1.2 区块链生态安全

目前涉及区块链安全的几大生态主要包括交易所、矿池、钱包、服务性网站等，我们在使用加密货币的过程中难免会将自己的资产托管到这些环节中，而这些涉及到数字货币交易与存储的地点也是以下几种攻击的重灾区。

交易所钱包被盗：主要是指中心化的交易所和钱包，去中心化交易所及钱包由于私钥在使用者手中，属于使用安全序列。通常中心化的交易所及钱包主要有冷钱包及热钱包，若私钥保存不当都存在被黑客窃取的可能。另一种被盗情形是指黑客通过修改交易所后台数据，给自己账户增加币然后提币的方式盗取。

交易所、矿池、网站被 DDoS 攻击：即通过大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。该攻击主要目的是为了拒绝合法用户正常使用网络。区块链面对 DDoS 攻击通常采用手续费的方式让矿工优先打包高手续费的交易。而链外相关的生态所搭建的网站中，也有可能遭受类似的攻击。

DNS 劫持：是指在劫持的网络范围内拦截域名解析的请求，分析请求的域名，把审查范围以外的请求放行，否则返回假的 IP 地址或者什么都不做使请求失去响应，其效果就是对特定的网络不能访问或访问的是假网址。

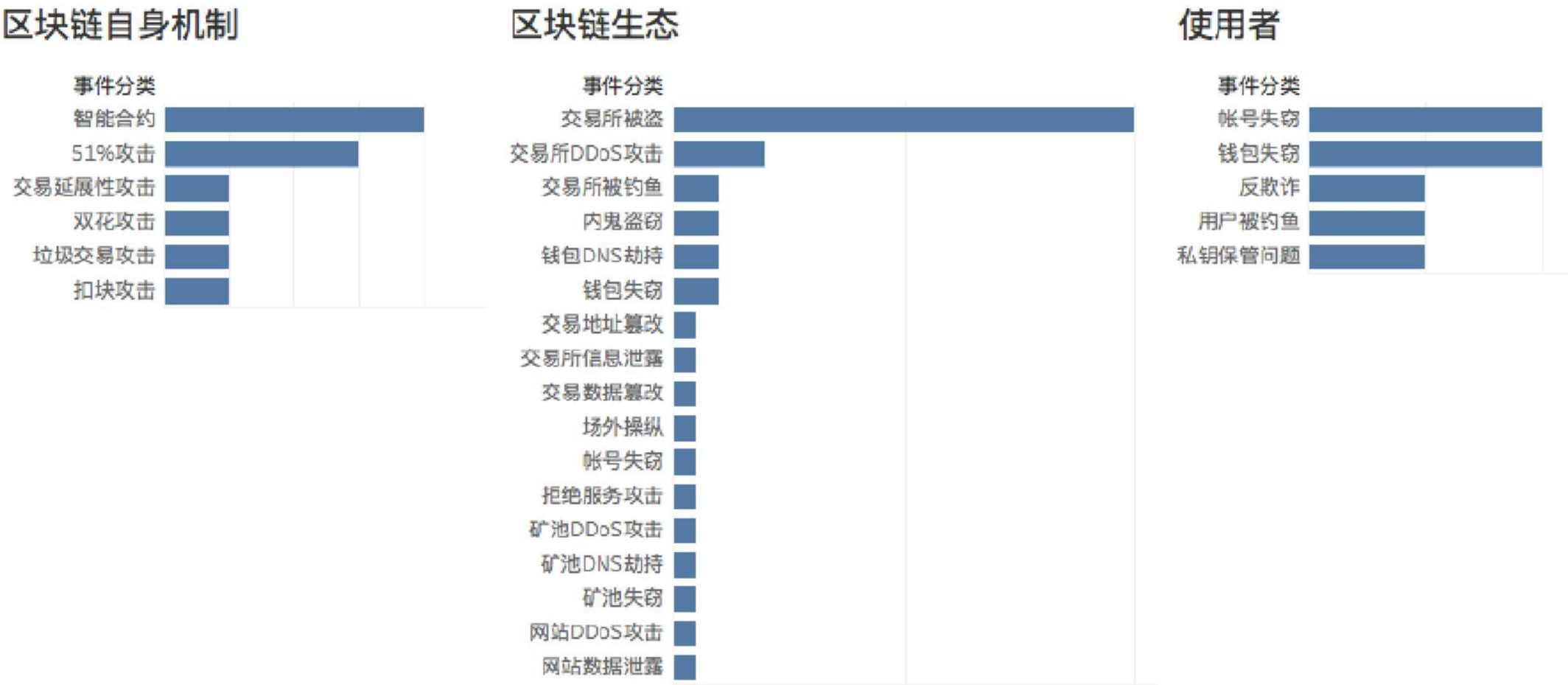
### 2.1.3 区块链使用安全

使用安全是指个人在使用和交易数字货币的过程中遭遇的数字货币私钥、账号被窃取的情形。造成这种情况的主要原因在于被钓鱼、植入木马、私钥保管不删、被欺诈等情况造成。

# 2.2 安全事件

## 2.2.1 安全事件统计

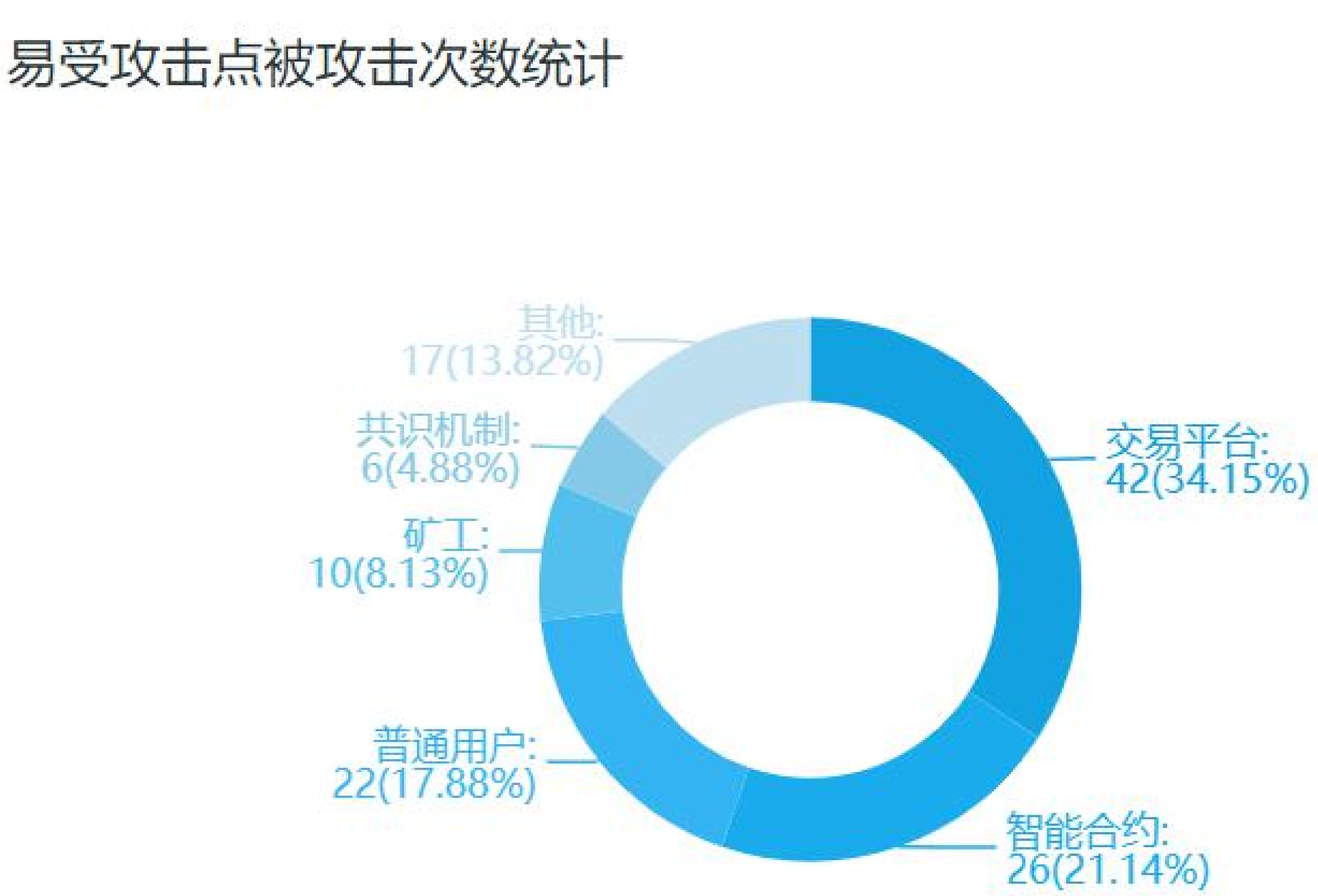
加密数字货币一经诞生，安全性就是人们关注的焦点，遗憾的是各类重大安全事件层出不穷。尤其是总市值不断增大，数字货币种类逐渐繁多，区块链生态进一步丰富，给了攻击者越来越多的突破口，每年的涉案金额也在不断增多。总的趋势是，随着数字虚拟货币参与者的增加，各种原因导致的安全事件也显著增加。



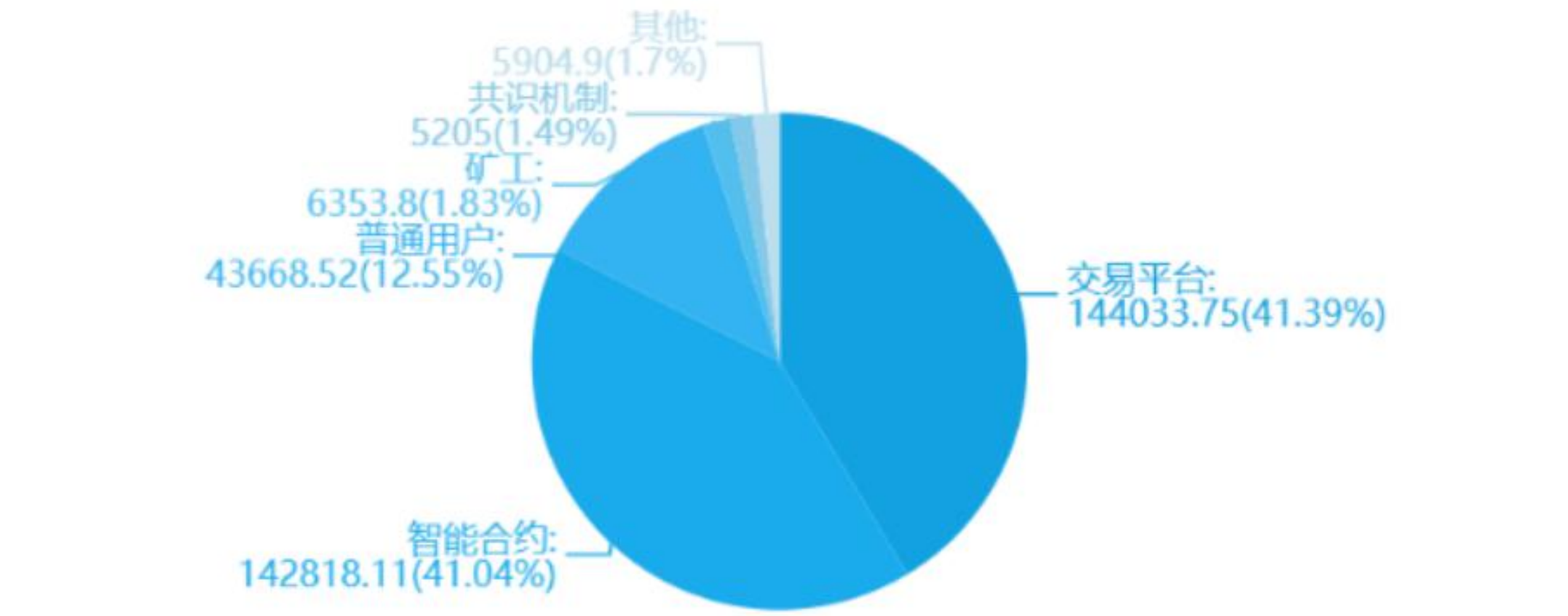

根据对近年来区块链安全事件的调查统计显示，因区块链自身机制所导致的安全问题主要发生在智能合约与 51%攻击上。其中利用合约漏洞盗币中具有代表性的案例是 2016 年 The DAO 事件以及 BEC 和 Smartmesh 合约出现重大安全漏洞引发的黑客盗币。这部分所造成的损失大约占 12.5 亿美元。

在区块链生态中所发生的安全问题则主要集中在交易所被盗方面。一方面是以为交易所在币圈群体覆盖范围更加广泛，另一方面则是交易所所汇集的资金更为庞大，对黑客有诱惑力。这部分所造成的资金损失达 14.2 亿美元。

因使用者自身原因而造成的安全事故中，主要体现在账号失窃与钱包失窃中。这主要是由于大部分数字货币的持有者安全意识不强，对于私钥没有一个正确的概念以及不能妥善保管账号、私钥所致。这部分造成的损失达 0.56 亿美元。

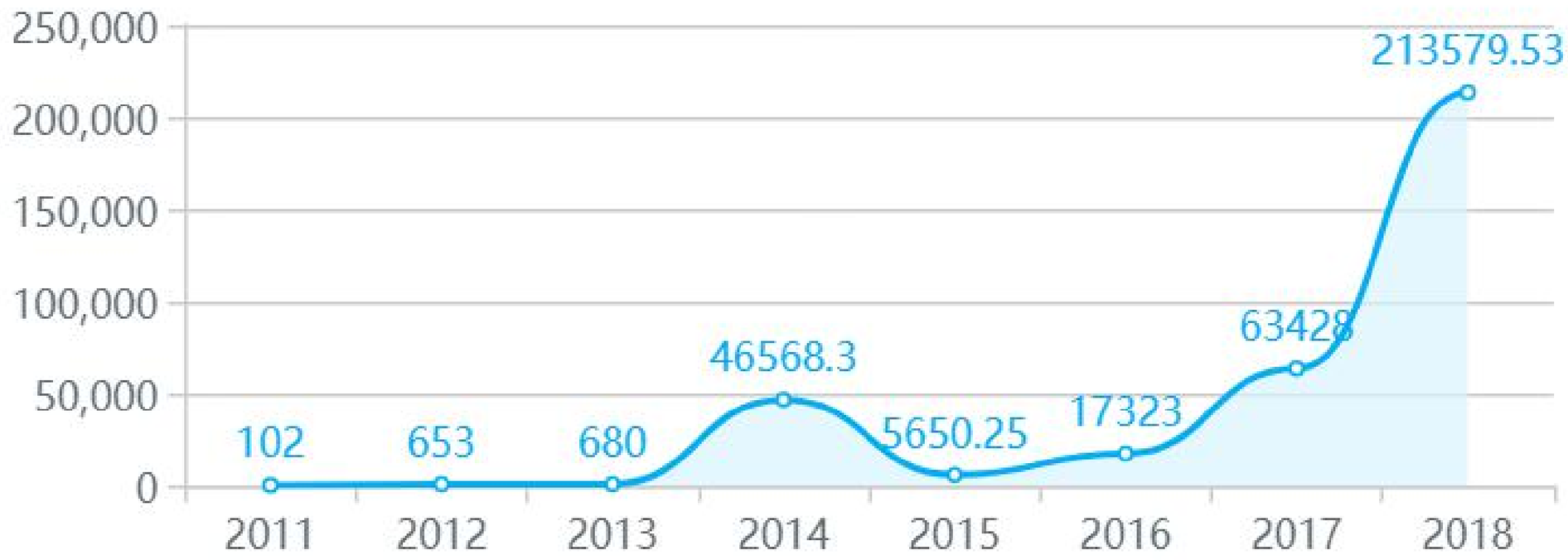



从区块链安全网提供的数据显示，最易受攻击的板块主要集中在交易平台、智能合约、普通用户上，分别达 42、26、22 次，占比 34%、21%、18%。




这其中，又以交易平台和智能合约所遭受的损失居多，二者相加共计 28 亿美元，均占比 41%。

安全事件造成的经济损失趋势(万美元)




从近几年区块链安全事件统计的图表中可以得出，随着数字货币参与者人数的增加，区块链项目种类增多，所引发的安全事件以及所造成的经济损失也在显著增加。早期区块链安全事故年均 10 起以下，而在 2017 年达到了 15 起，2018 年未过完已攀升到 75 起。因安全问题所造成的经济损失也达到了 21 亿美元。

## 2.2.2 重大安全事件摘要：

行业发展至今，众多安全事故给从业人员以及投资者造成了巨大损失，以下是近年来行业中比较有影响力的区块链安全事件梳理：

- 2011 年 6 月：Mt.Gox 安全漏洞被黑，泄露大量数据，比特币价格一度跌至 1 美分
- 2014 年 2 月：Mt.Gox 被黑客攻击，被盗 85 万枚比特币，导致其破产，损失约 3.6 亿美金
- 2014 年 3 月：美国数字货币交易所 Poloniex 被盗，损失 12.3%的比特币
- 2015 年 1 月：Bitstamp 交易所被盗 1.9 万枚比特币，当时价值 510 万美元
- 2016 年 6 月：以太坊链上的 The DAO 智能合约遭到攻击，涉及到总额 300 多万个以太币，约合 6000 多万美金
- 2016 年 8 月：知名比特币交易平台 Bitfinex 被盗 12 万枚比特币，价值 18 亿美元
- 2017 年 6 月：韩国交易平台 Bithumb 被黑客入侵，受损账户损失数十亿韩元
- 2018 年 4 月：BEC 及 SMT 出现重大合约安全漏洞，导致价格大跌
- 2018 年 5 月：比特黄金 BTG 遭 51%算力攻击，损失 1860 万美元

# 3. 行业中坚力量分析

对于行业中频发的安全问题，处于对这个领域的需求，行业中一些安全服务机构也逐渐发展壮大，针对安全问题提供的服务也日趋专业化。目前，国内外几大服务于区块链安全的公司与团体主要包括慢雾科技、知道创宇、360 区块链安全、Certik 等机构。

## 3.1 知道创宇

知道创宇成立于 2007 年，由数位国际顶尖的安全专家创办，并拥有近百位国内一线安全人才的核心安全研究团队。知道创宇是国内最早提出云监测与云防御理念的网络安全公司，经过多年的积累，利用在云计算及大数据处理方面的行业领先能力，可为客户提供具备国际一流安全技术标准的可视化解决方案，提升客户网络安全监测、预警及防御能力，于 2015 年获得腾讯大范围战略投资。

### 云防护

抗D保（DDoS、CC防御）
创宇盾（云WAF）
加速乐（CDN加速）

### 智能合约审计

国内顶级白帽子团队对智能合约中交易、故障、隐私等风险进行源码审计

### 智能钱包安全

采用国际EAL5+认证芯片，通过分层确定性的方式对秘钥进行多层防护，确保钱包安全

### 算力安全监控

对算力设备进行多维度安全防护和监测，实时报告异常操作

### 安全服务

威胁感知、漏洞管理、代码审计、渗透测试、系统加固、移动安全、应急响应、威胁情报

### 业务反欺诈

全网监测，多平台实施拦截，全球快速封停钓鱼网站，精准识别羊毛党

作为一家综合性安全服务公司，区块链业务只是知道创宇业务中的一环，其中包括云防护、智能合约审计、智能钱包安全、算力安全监控、安全服务、业务反欺诈等方面。并且与火币、Bitmain、ViaBTC 等行业翘楚建立了合作关系。

## 3.2 链安科技

成都链安科技有限公司，专注区块链安全领域，总部位于成都。由电子科技大学杨霞教授和郭文生教授共同创建，团队核心成员由 30 多名来自海外知名高校和实验室（CSDS、耶鲁、UCLA）留学经历的副教授、博士后、博士、硕士及阿里、华为等知名企业精英组成。其核心技术为形式化验证，该团队使用此技术为航天、军事等领域的安全关键系统提供多年的形式化验证服务，是国内唯一一家将此技术应用到区块链安全领域的公司。


链安科技提供的服务主要以安全审计为主，另外还包括智能合约的开发。其 VaaS “一键式”智能合约安全验证平台是全球首个同时支持 EOS、以太坊区块链智能合约的自动形式化验证平台，具有验证效率高、自动化程度高、人工参与度低、易于使用、支持多种合约开发语言、可支持大容量区块链底层平台等特点。

链安科技团队的技术以及专业化程度得到了业内深度认可。目前，链安科技的合作伙伴不仅包括分布式资本、CSDN，还有 OKEx、Huobi、Kucoin 等知名交易所以及 BTM、ONT 等优质区块链项目。

## 3.3 慢雾科技

厦门慢雾科技有限公司，专注区块链生态安全，总部位于厦门，由一支拥有十多年一线网络安全攻防实战的团队创建，团队成员曾为 Google、微软、W3C、公安部、腾讯、阿里、百度等输出过安全能力，团队成员多项成果也曾进入过 Black

Hat 等全球黑客大会。慢雾科技的核心能力包括：安全审计、安全顾问、防御部署、威胁情报等。慢雾科技已经为全球多家交易所、钱包、链、智能合约等做了安全审计与防御部署，并通过独有的地下黑客风向标追踪引擎，持续为合作公司及国家相关部门提供威胁情报。


慢雾科技的业务布局

在 2018 年上半年区块链安全漏洞频发的时期，慢雾团队发现以及检测到了多个安全漏洞，其中包括因以太坊生态缺陷导致的亿级代币盗窃大案、USDT 虚假转账案、以太坊假充值案等。慢雾科技以其精湛的技术与良好的行业口碑，与区块链行业多家知名机构与项目方建立了合作关系，其中包括：imtoken、OKEx、火币安全、ONTology、Vechain、引力区、Whormhole 等。

# 3.4 360 区块链安全

360 作为全国最大的互联网安全企业，推出了 360 区块链安全板块，目前主要为钱包、交易所、矿池、智能合约、EOS 超级节点五大板块提供安全服务。在 EOS 主网上线前，向 blockone 公司提供了 EOS 重大漏洞避免了巨大损失。


# 3.5 Certik

CertiK 是一家用形式化验证为智能合约和区块链应用提供最先进安全性服务的公司。凭借团队精湛的技术以及更加专业化的服务，得到了业内很多重要机构的认可。目前已与比特大陆、币安、丹华资本、FBG 资本以及唯链、小蚁、本体、星云、量子、IOST、AELF 等知名项目建立合作关系。

# 4.行业安全板块

综合对比各大区块链服务机构所提供的业务板块，主要集中在以下几部分。

## 4.1 交易所钱包安全审计

在区块链行业安全板块中，交易所安全不容忽视，因为交易所平均每天的交易额都是数以亿计，然而交易平台背后的经营者能力与平台的自身的安全性并没有很好的保障。交易所安全审计涉及到大量投资者以及平台项目方的资产安全。

区块链的钱包指的是存储区块链资产的地址和私钥的文件。钱包也诸多安全风险例如：钱包客户端 RPC API 风险 ，私钥窃取，钱包软硬件漏洞攻击，在线钱包账号窃取等。人们通常倾向于将自己的大额不用于流动的数字资产存放在钱包中，因此钱包安全审计也尤为重要。


交易所钱包安全审计项
App 安全审计
App 缓存安全检测
通信加密检测
代码反编译检测
文件存储安全检测
权限检测
认证绕过测试
默认口令测试
权限提升测试
Hash 健壮性测试
密码重置测试
认证与授权审计
安全问答测试
跨站脚本（XSS）测试
XXE 实体注入测试
SSRF 漏洞测试
输入安全审计
命令执行注入测试
模板注入测试
SQL 注入测试
完整性测试
请求伪造测试
接口频率限制测试
恶意文件上传测试
应用误用防护测试
业务逻辑审计
超时检测
工作流程绕过测试
身份鉴别管理审计
接口安全测试
业务安全检测
邮件服务探测
子域探测
人员组织结构采集
端口服务组件指纹采集
开源情报采集
证书信息采集
人员隐私泄露发现
会话管理审计
跨站点请求伪造测试
Cookies 属性测试
登出功能测试
会话令牌泄露测试
会话超时测试
会话令牌重载测试
会话固定测试
会话管理绕过测试
服务端安全配置审计
弱口令及默认口令探测
文件扩展名解析测试
备份、未链接文件测试
管理后台发现
应用平台配置管理测试
网络基础设施配置测试
CDN 服务探测
密码学安全审计
加密传输层防护测试
安全部署测试
HTTP 严格传输测试
非加密信道传输敏感数据测试
节点安全审计
用户注册过程测试
角色定义测试
弱用户名策略测试
帐户枚举测试
节点配置安全检测
节点数据同步检测
帐户权限变化测试
节点开源代码
节点通信安全
节点交易

# 4.2 链安全审计

对于新开发的区块链，包括各种公链，联盟链，私链， 在链上的审计尤为重要，链上的漏洞对于整个链生态影响极大，不同于在已有链上发布的某个智能合约。链安全审计主要包括：节点配置安全审计、节点通讯安全审计、合约虚拟机安全审计、节点共识安全审计、官方钱包安全审计等。

# 4.3 智能合约安全审计

智能合约安全时间频出，软件工程师创造一个完全无误差的代码是不可能的，程序员总存在疏忽的地方，智能合约安全审计成就完美合约。目前各区块链安全机构提供的智能合约安全审计项如下图：

## 4.4 安全顾问

很多创业公司都没有安全部门，也比较少有安全意识，区块链领域也不例外。所以需要专业安全团队对整个产品做一次评测，安全团队对客户产品围绕着几大环节（开发过程、运维过程，技术组件选型，现有已开发的系统，产品整体架构及操作过程，关键技术岗位人员组成状况，办公内网拓扑及终端状况，当前整体风控体系状况，团队协作平台）进行针对性的安全问答，并给出相应的安全加固建议。同时对客户的安全加固过程进行跟踪，确保安全加固建议准确落实。

## 4.5 安全运营

为了保证系统高可用且安全，还需在日常安全运营上面下功夫，主要是包括以下几个方面：

- 详尽的访问控制，根据实际业务需求判断访问权限合理性。
- 全面的日志审计，根据日志对重要系统操作行为做审计。
- 及时的告警处置，对日常告警做专业性判断。
- 需要日常漏洞管控，对已知漏洞给予专业性处理建议。
- 对员工进行安全培训，提供安全意识、安全开发等培训。

# 4.6 威胁情报

同传统互联网的安全技术发展路线类似，区块链安全行业也开始引入态势感知，或者称为威胁情报。随着区块链越来越多的进入实际应用，在区块链上做态势感知（威胁情报）已经成为一个非常迫切的需求。在区块链上进行做业务，预防的重要性要远超传统信息安全中的预防。

传统安全领域通常认为威胁情报就是收集、评估和应用关于安全威胁、威胁分子、攻击利用、恶意软件、漏洞和漏洞指标的数据集合，可用于主体制定面对威胁或危害时的应急计划。

在区块链领域的威胁情报，除了传统的上述诸多内容外，还包括了链上数据分析和区块链中的 P2P 网络数据分析这些专用的技术手段。对于使用联盟链的企业，其所应用的区块链系统往往是位于企业内部网络的，或者是和互联网有防火墙隔离的专用网络。企业除了应及时关注所使用的区块链软件的安全性外，还应该部署一些用于监控链上数据和区块链 P2P 网络数据的软件。在对这些数据，尤其是失败的没有上链的数据，进行智能的分析，往往能够在真正的大的安全事件出现之前，寻找到蛛丝马迹，发出告警提醒企业对其进行防范。

# 4.7 漏洞赏金

由于区块链网络的匿名性和“无法追踪的交易”特性，区块链上丢失的资金是不可能收回的。越来越多的公司开始花钱寻找漏洞，以揭露其各自网络上可能存在的漏洞。这鼓励负责任地披露网络中的潜在威胁，这将有助于解决区块链网络的安全问题。

要想让加密货币以及更广泛的区块链技术和公司的发展和繁荣，对独立黑客正在进行的安全审查是必须的。由于大量黑客社区正在寻找安全漏洞，因此很有可能及时找到并解决这些漏洞。

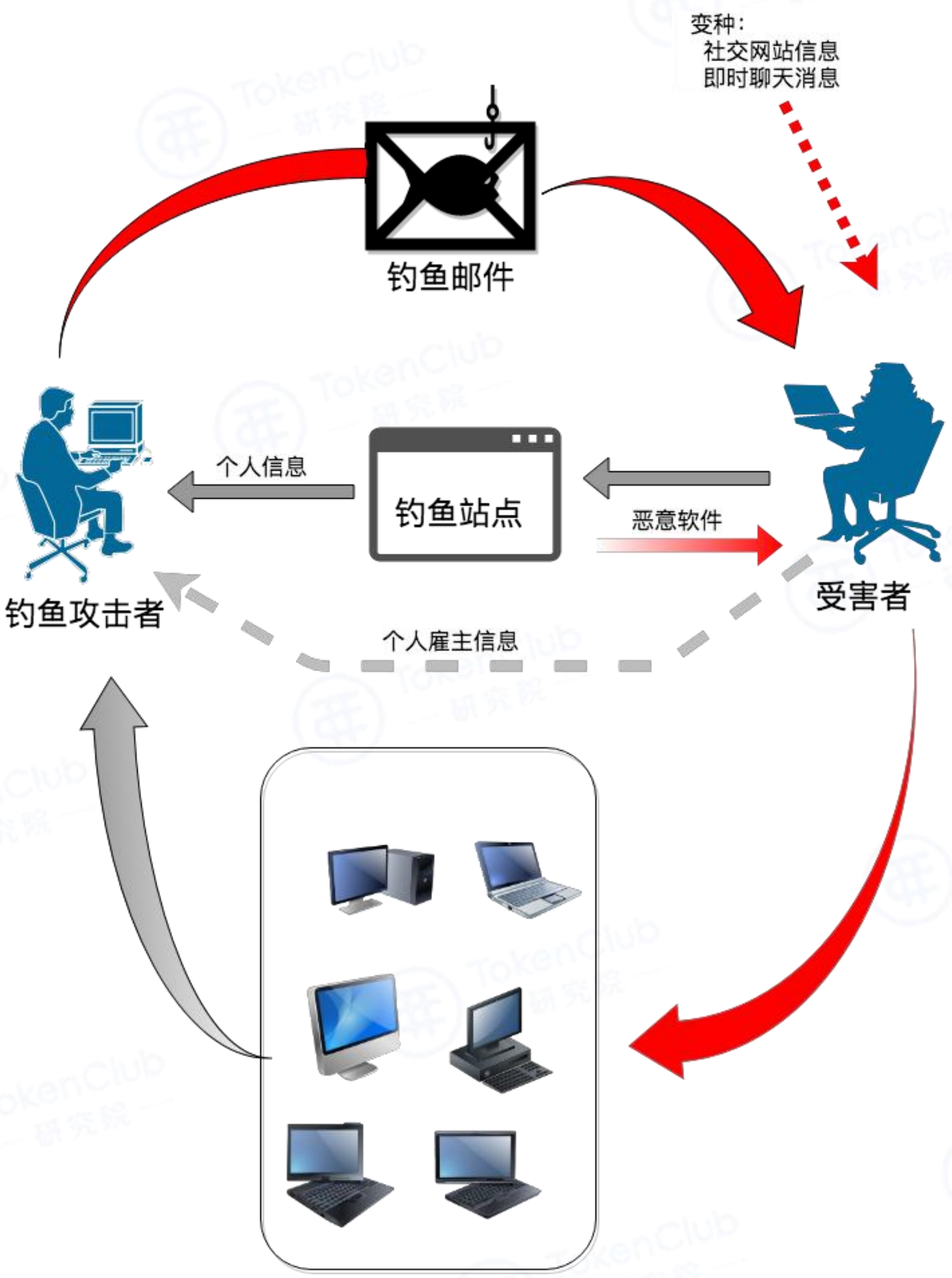
漏洞赏金计划让黑客有机会合法地找到网络中的漏洞并获得奖励。它还有一个额外的好处，就是让公司对其网络上的违规行为负责。漏洞赏金计划对投资者和公司都是一种解脱。这减少了潜在的黑客攻击的可能性，并使公司能够识别他们自己的网络中的威胁，增加加密爱好者之间的信任。

# 5.攻防技术分析

传统互联网的攻击手段、防御手段繁多，比如钓鱼，DDOS 等。相对传统互联网，区块链攻击手段又多了一些，主要是围绕区块链技术原理特有的攻击，比如双花攻击，女巫攻击等。

## 5.1 钓鱼攻击

钓鱼攻击，是最为普遍的一种攻击方式，攻击者利用社会工程学手段来伪装成可以信任的人或机构，以获得用户名、密码和银行卡明细等个人敏感信息的犯罪诈骗过程。常用的攻击手段有链接监控，过滤器规避，网站伪造，电话网钓，WIFI 免费热点网钓，隐蔽重定向漏洞。




攻击场景主要包括:

- 利用近似域名+高度仿冒网站欺骗投资者。比如 unicode 钓鱼手法。
- 利用电子邮件散步虚假信息，如 ICO 项目的收款地址更改通知等
- 在社交软件、媒体上散步钓鱼信息来欺诈投资者

在目前的互联网环境中，欺诈随处可见，这种攻击手段在区块链应用上也同 样受用。攻击者可以伪造某个钱包客户端，无论从界面和操作上都可以做到和真 钱包没有区别，可能他们只是在你转账的时候窃取你的私钥信息或者在转账地址上动手脚，就可以轻易地偷偷窃取你的资产。

所以，客户端一定要在官网下载，并验证官网发布的客户端文件 hash 是否与下载的客户端文件 hash 一致。

## 5.2 拒绝服务攻击

这个类别比较广泛，由让用户在一段时间内或永久地在某些情况下使合约无法运行的攻击组成。这就可以永远地获取合约中的以太，就像 Parity 多重签名钱包第二次攻击事件一样。攻击情形：

- 通过外部操作循环中的数组。通常它出现在 owner 分配代币给投资者的情况下，使用 distribute()可以在示例合约中看到类似功能的情况：

```
contract DistributeTokens {
    address public owner; // gets set somewhere
    address[] investors; // array of investors
    uint[] investorTokens; // the amount of tokens each investor gets

    // ... extra functionality, including transfertoken()

    function invest() public payable {
        investors.push(msg.sender);
        investorTokens.push(msg.value * 5); // 5 times the wei sent
        }

    function distribute() public {
        require(msg.sender == owner); // only owner
        for(uint i = 0; i < investors.length; i++) {
            // here transferToken(to,amount) transfers "amount" of tokens to t
            transferToken(investors[i],investorTokens[i]);
        }
    }
}
```

此合约中的 investors 数组大小没有限制，所以攻击者可以创建很多账户，使得 investors 数组变得非常大，以致于运行 for 循环所需要的 gas 超过了区块的 gas limit，使用 distribute()方法不可用。

- 所有者操作 - 另一种常见模式是 owner 在合约中拥有特定权限，并且必须执行一些任务才能使合约进入下一个状态。例如，ICO 合约要求所有者 finalize() 签订合约，然后允许 token 可以交易，即

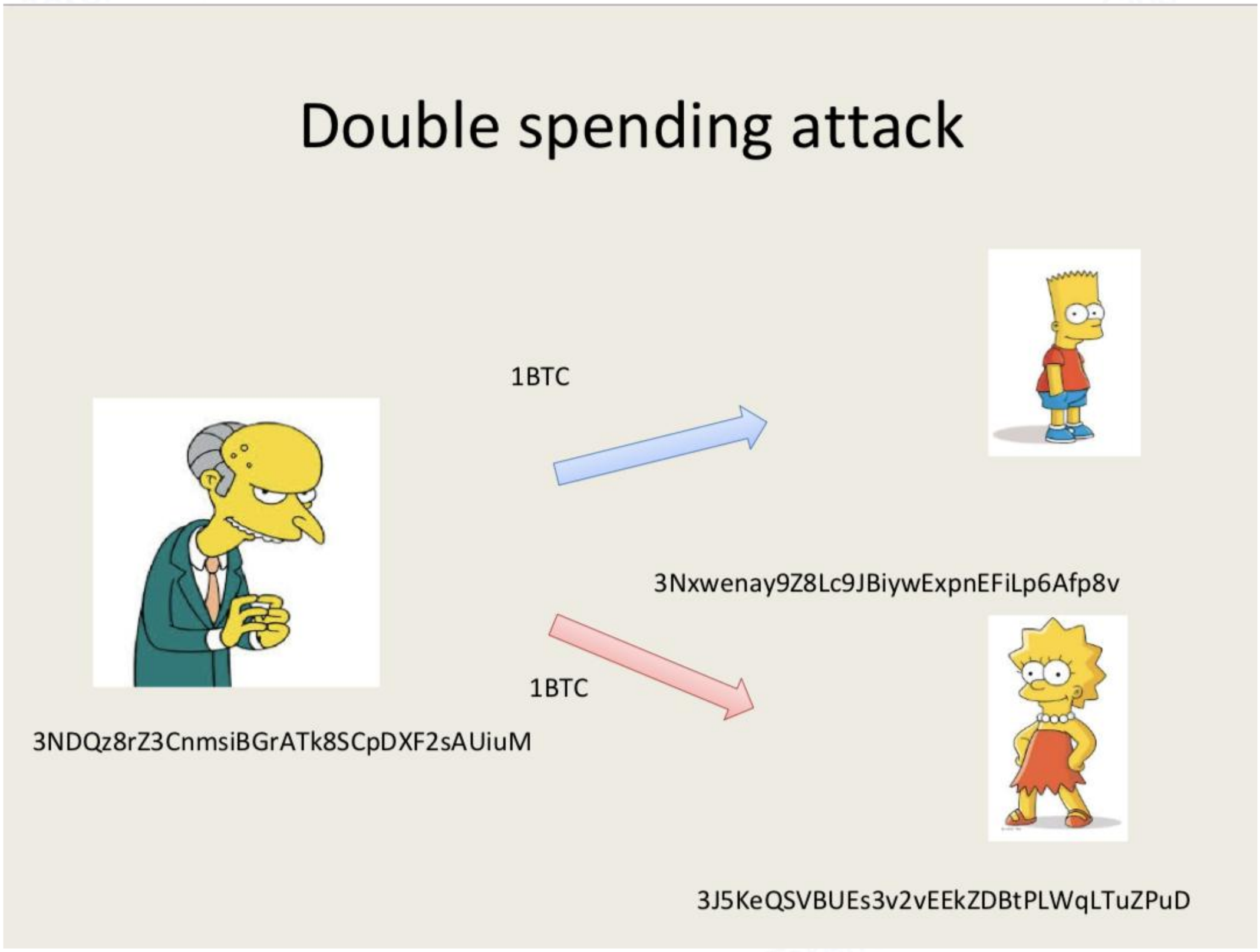
```
bool public isFinalized = false;
address public owner; // gets set somewhere

function finalize() public {
    require(msg.sender == owner);
    isFinalized == true;
}

// ... extra ICO functionality

// overloaded transfer function
function transfer(address _to, uint _value) returns (bool) {
    require(isFinalized);
    super.transfer(_to,_value)
}

...

```

在这种情况下，如果特权用户丢失其私钥或变为非活动状态，则整个 token 合约变得无法操作。如果 owner 无法调用 finalize()不可以转让代币，即令牌生态系统的整个操作取决于一个地址。

- 基于外部调用的进展状态 - 合约有时被编写成为了进入新的状态需要将以太网发送到某个地址，或者等待来自外部来源的某些输入。这些模式可能导致 DOS 攻击，当外部调用失败时，或由于外部原因而被阻止。在发送以太的例子中，用户可以创建一个不接受以太的契约。如果合约需要将以太送到这个地址才能进入新的状态，那么合约将永远不会达到新的状态，因为以太永远不会被送到合约。

# 5.3 双花攻击

双花攻击，是指将一个代币通过多次支付手段发起的攻击。发起双花攻击的方式有很多，除了人们熟知的 51%攻击，还包括种族攻击、芬妮攻击、Vector 76 攻击、替代历史攻击等形式。



### 5.3.1 种族攻击

这种攻击方式主要通过控制矿工费来实现双花，攻击对象主要是那些在面对 0 确认（未确认）的交易便立刻进行付款的商家。

攻击者把一定数量的 token 发给一个商家，我们命名为分支 A。如果商家接受 0 确认，那么攻击者就会再把这笔 token 发给自己的一个钱包，并加了较高矿工费，我们命名为分支 B。不过，攻击者在发给自己的这笔交易中，加了较高的矿工费，从而提高被矿工打包的概率（间接提高了攻击成功率）。如果攻击者发给自己的这笔交易被提前打包，这时候这笔交易就先于发给商家的交易，也就是分支 B 的长度超过分支 A 的长度，分支 A 上的交易就会被回滚。对于攻击者来说，通过控制矿工费，就实现了同一笔 token 的“双花”。

### 5.3.2 芬妮攻击

这种攻击方式主要是通过控制区块的广播时间来实现双花，攻击对象是接受 0 确认的商家。

攻击者挖到一个数据块。在区块中，他打包了地址 A 到地址 B 的交易信息。两个地址都是工具者的，但他不会立即广播此区块。相反，他立即找到一个商家，并使用地址 A 向商家的地址 C 付款。如果商家接受 0 确认。接着他广播他之前的区块，他的交易将优先于对商家的交易，于是对商家的付款交易作废。

## 5.3.3 Vector76 攻击

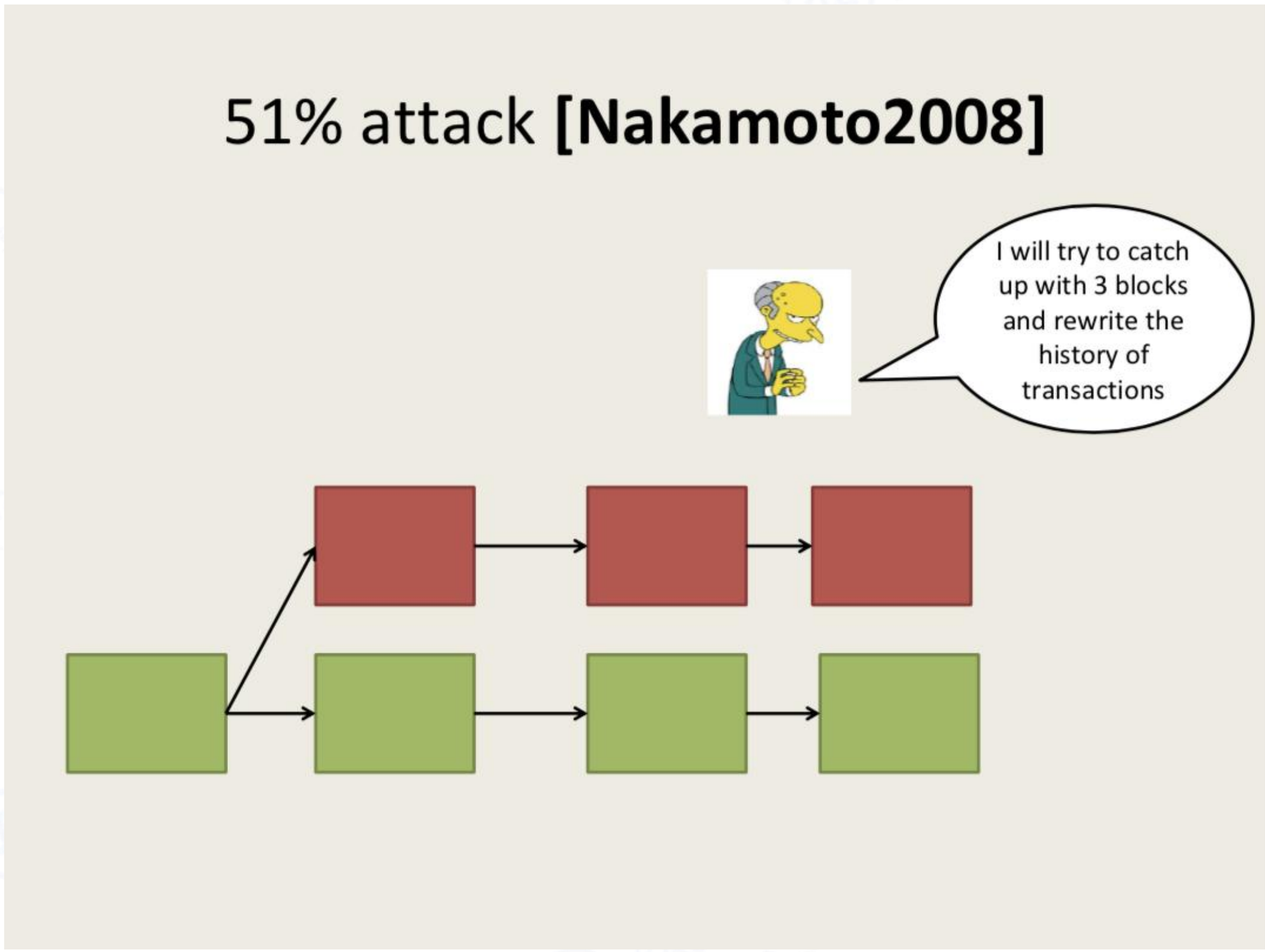
Vector76 攻击，是种族攻击和芬尼攻击的组合，又称“一次确认攻击”，也就是交易即便有了一次确认，交易仍然可以回滚。如果电子钱包满足以下几点，Vector76 攻击就容易发生。这几点即钱包接受一次确认就支付；钱包接受其它节点的直接连接；钱包使用静态 IP 地址的节点。

## 5.3.4 替代历史攻击

即使商家等待一些确认，这种攻击也有机会成功，但风险较高。攻击者向商家提交支付的交易，同时私下挖掘其中包含欺诈性 双重支出交易的分支。等待 n 次确认后，商家发送产品。如果攻击者此 时碰巧找到 n 个以上的区块，他就会释放他的分支并重新获得他的硬币。如果商家在等待交易确认，alternative history attack 就有机会发生，当然，这需要攻击者有较高的算力，对于攻击者来说，会有浪费大量电力的风险。

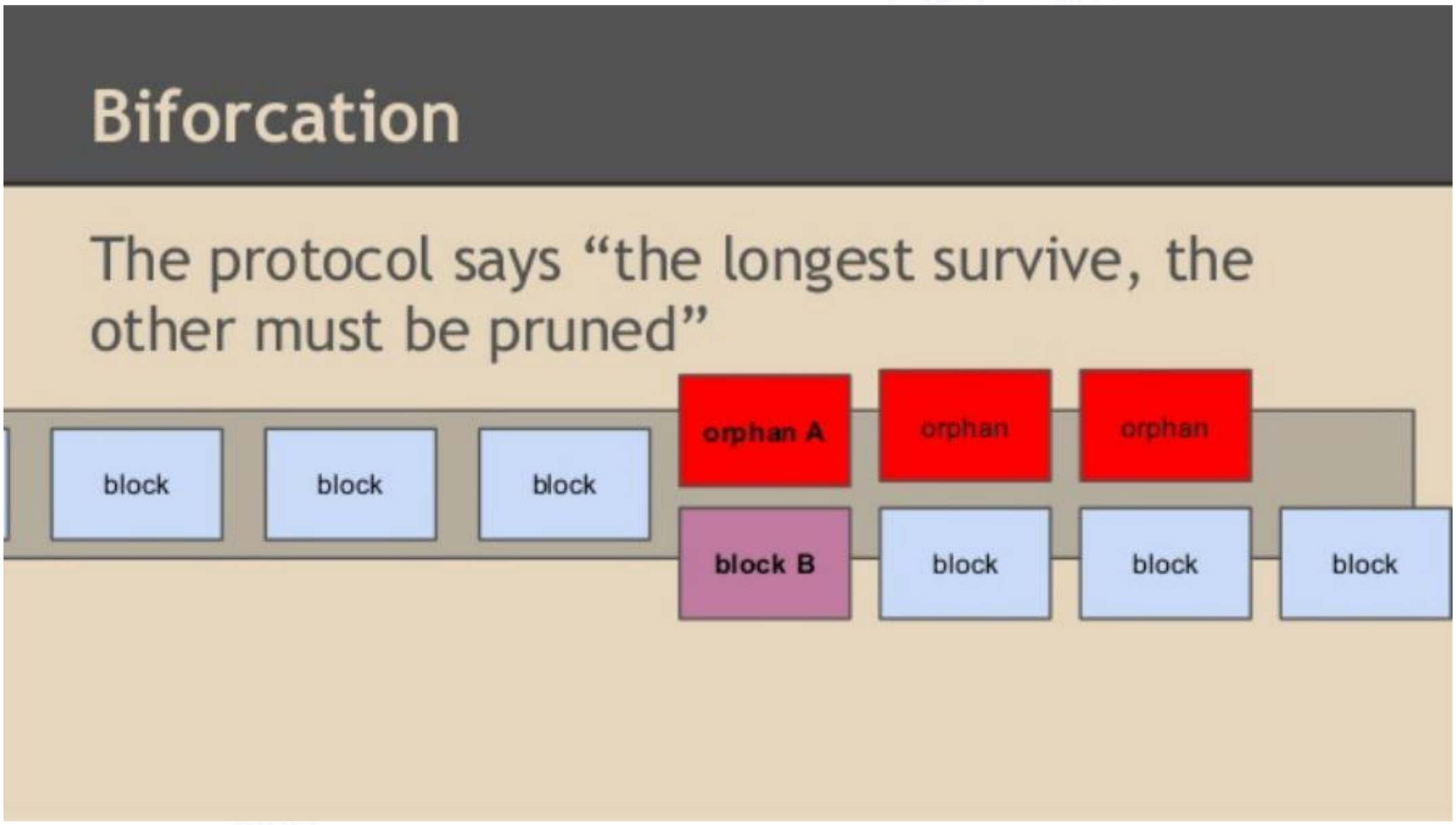
## 5.3.5 51%算力攻击

这种攻击是通过控制网络算力来实现双花。如果攻击者控制了网络中 50%以上的算力，那么在他控制算力的这段时间，他可以将区块逆转，进行反向交易，实现双花。




比如 Bitcoin Gold 发生的双花问题就属于 51%攻击。 攻击者控制 Bitcoin Gold 网络上 51%以上的算力，在控制算力的期间，他把一定数量的 BTG 发给自己在交易所的钱包，这条分支我们命名为分支 A。同时，他又把这些 BTG 发给另一个自己控制的钱包，这条分支我们命名为分支 B。

分支 A 上的交易被确认后，攻击者立马卖掉 BTG，拿到现金。这时候，分支 A 成为主链。然后，攻击者在分支 B 上进行挖矿，由于其控制了 51%以上的算力，那么攻击者获得记账权的概率很大，于是很快，分支 B 的长度就超过了主链，也就是分支 A 的长度，那么分支 B 就会成为主链，分支 A 上的交易就会被回滚（回滚指的是程序或数据处理错误，将程序或数据恢复到上一次正确状态的行为）。




也就是说，分支 A 恢复到攻击者发起第一笔交易之前的状态，攻击者之前换成现金的那些 BTG 又回到了自己手里。当然，这些 BTG 就是交易所的损失了。最后，攻击者把这些 BTG，发到自己的另一个钱包。就这样，攻击者凭借 51%以上的算力控制，实现同一笔 token 的“双花”。

## 5.4 整数溢出攻击

整数溢出有向上溢出和向下溢出，在传统安全领域中，整数安全与数据模型和整数运算支持的运算符相关，其中数据模型又跟处理器架构体系和操作系统平台相关。模型如图：

通用处理器的数据模型

| 数据类型 | 8086 | x86-32 | 64 位 Windows | SPARC-64 | ARM-32 | Alpha | 64 位 Linux、FreeBSD、NetBSD 和 OpenBSD |
|---|---|---|---|---|---|---|---|
| char | 8 | 8 | 8 | 8 | 8 | 8 | 8 |
| short | 16 | 16 | 16 | 16 | 16 | 16 | 16 |
| int | 16 | 32 | 32 | 32 | 32 | 32 | 32 |
| long | 32 | 32 | 32 | 64 | 32 | 64 | 64 |
| long long | N/A | 64 | 64 | 64 | 64 | 64 | 64 |
| pointer | 16/32 | 32 | 64 | 64 | 32 | 64 | 64 |

C 语言中容易引发整数安全问题的运算符简要罗列如下图：

异常情况

| 运算符 | 异常情况 | 运算符 | 异常情况 | 运算符 | 异常情况 | 运算符 | 异常情况 |
|---|---|---|---|---|---|---|---|
| + | 溢出，回绕 | -= | 溢出，回绕，截断 | << | 溢出，回绕 | < | 无 |
| - | 溢出，回绕 | *= | 溢出，回绕，截断 | >> | 无[a] | > | 无 |
| * | 溢出，回绕 | /= | 溢出，截断 | & | 无 | >= | 无 |
| % | 溢出 | <<= | 溢出，回绕，截断 | ^ | 无 | == | 无 |
| ++ | 溢出，回绕 | >>= | 截断[a] | ~ | 无 | != | 无 |
| -- | 溢出，回绕 | &= | 截断 | ! | 无 | && | 无 |
| = | 截断 | \|= | 截断 | 一元 + | 无 | \|\| | 无 |
| +=[a] | 溢出，回绕，截断 | ^= | 截断 | 一元 - | 溢出，回绕 | ?: | 无 |

用 solidity 开发智能合约的整数安全场景与上面类似。

场景示例：

➢整数向下溢出，比如下面的 withdraw() 函数，没有先判断 balances[msg.sender] 跟 _amount 的大小。当 balances[msg.sender] < _amount 导致整数向下溢出，从而可以让用户提现无限数量当 token。

```
function withdraw(uint _amount) {
    require(balances[msg.sender] - _amount > 0);
    msg.sender.transfer(_amount);
    balances[msg.sender] -= _amount;
}
```

➢整数向上溢出，比如下面的 transfer( ) 函数，容易向上溢出。

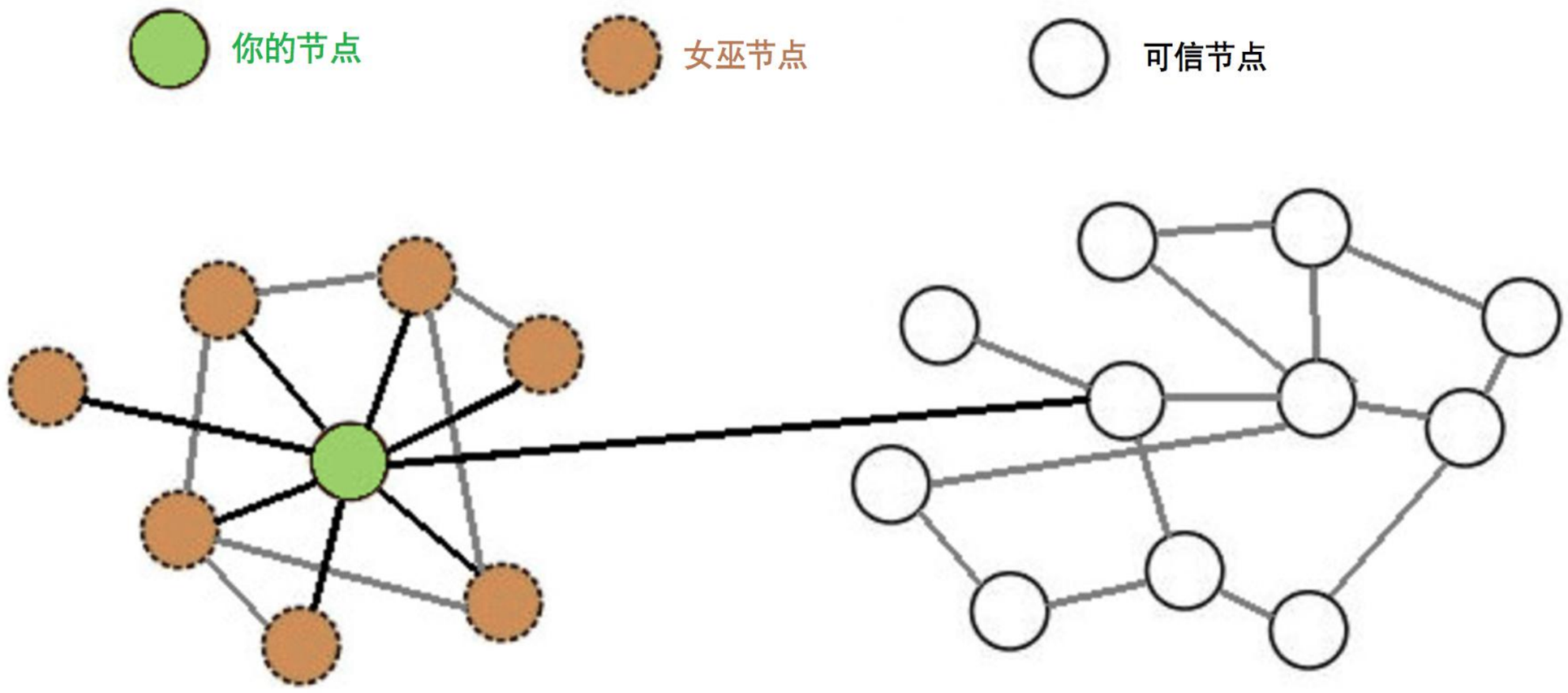
```
function transfer(uint _amount) {
    require( _amount > 0);
    balances[msg.receiver] += _amount;
}
```

➢采用了即将被弃用的 var 关键字。 因为 var 将自己变为包含指定数值所需的最小数据类型,所以它变成一个 uint8 类型来保存数值 0。如果循环迭代超过 255 次，它将在执行过程耗尽 gas 并且永远达不到该数值：

```
for (var i = 0; i < somethingLarge; i ++) {
    // ...
}
```

# 5.5 女巫攻击

解释：在 Sybil 攻击中，攻击者通过创建大量假身份来破坏 P2P 网络的信誉系统，用他们来造成更大影响。在 P2P 网络中的节点可以访问本地资源，而一个节点与本地资源的映射关系呈现出身份，节点会在 P2P 网络中广播自己的身份；然而多个身份可以对应一个节点，换句话说身份与节点的映射是多对一的。P2P 网络中的节点使用多个身份来实现数据冗余，资源共享，可靠性和完整性。女巫攻击是攻击数据冗余机制的一种有效手段。如果网络中存在一个恶意节点，那么同一个恶意节点可以具有多重身份，原来需要备份到多个节点的数据被欺骗地备份到了同一个恶意节点（该恶意节点伪装成多重身份），这就是女巫攻击。

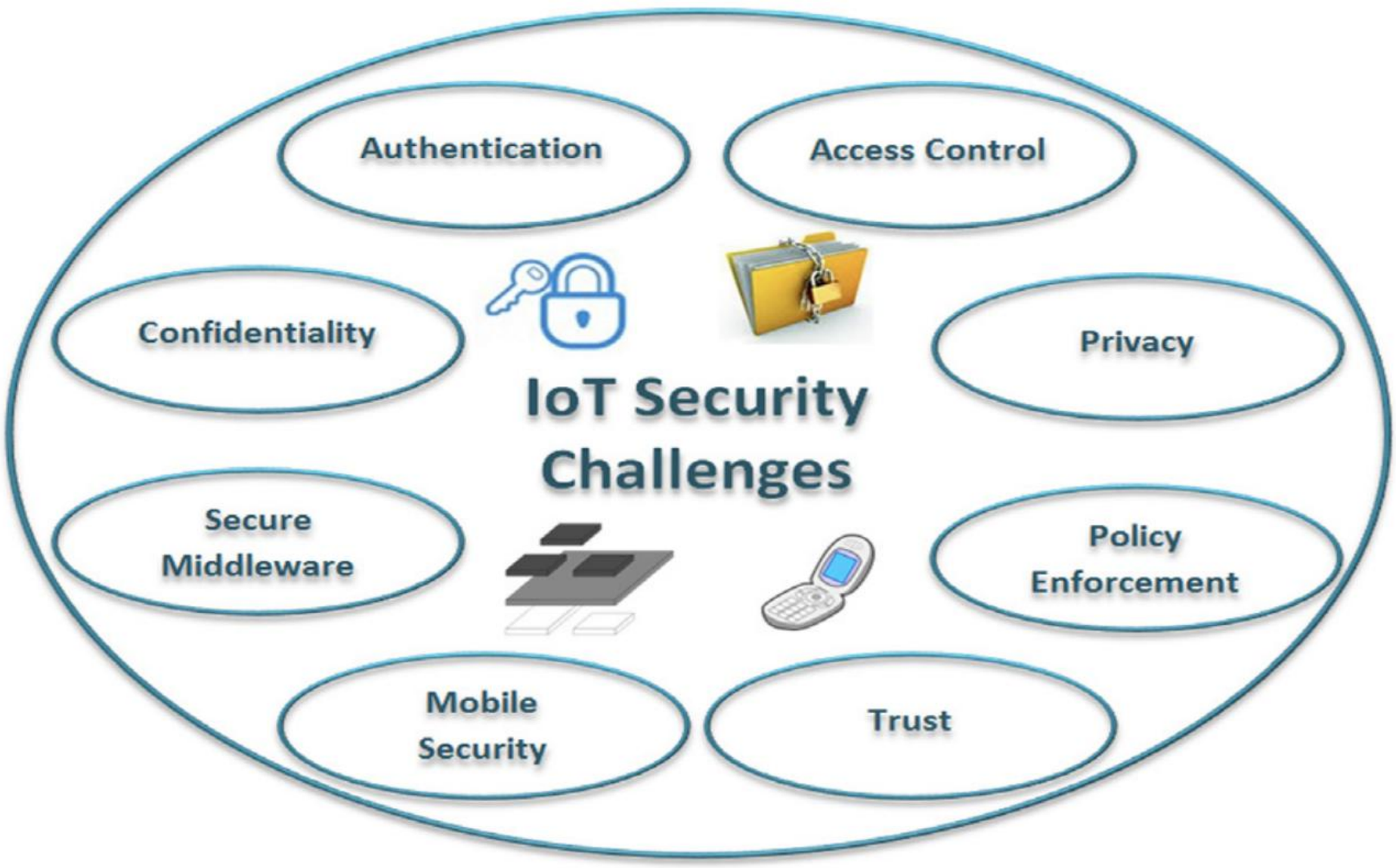



解决方法：使用身份认证来防范女巫攻击，POW 证明；基于第三方的身份认证：每加入一个新的节点都需要与某一个可靠的第三方节点进行身份验证；纯分布式的身份认证：每加入一个新的节点都需要获得当前网络中所有可靠节点的认证，这种方法采用了随机密钥分发验证的公钥体制的认证方式，需要获得网络中大多数节点的认证才能加入该网络。

# 6. 区块链安全行业应用

由于区块链自身设计机制上已包含有一些安全保护，比如数据不可以攥改，共识机制等。围绕区块链自身安全机制可以在安全行业做很多安全应用，比如设备身份识别，去中心化的公钥基础设施等。

## 6.1 使用身份验证保护边界设备安全



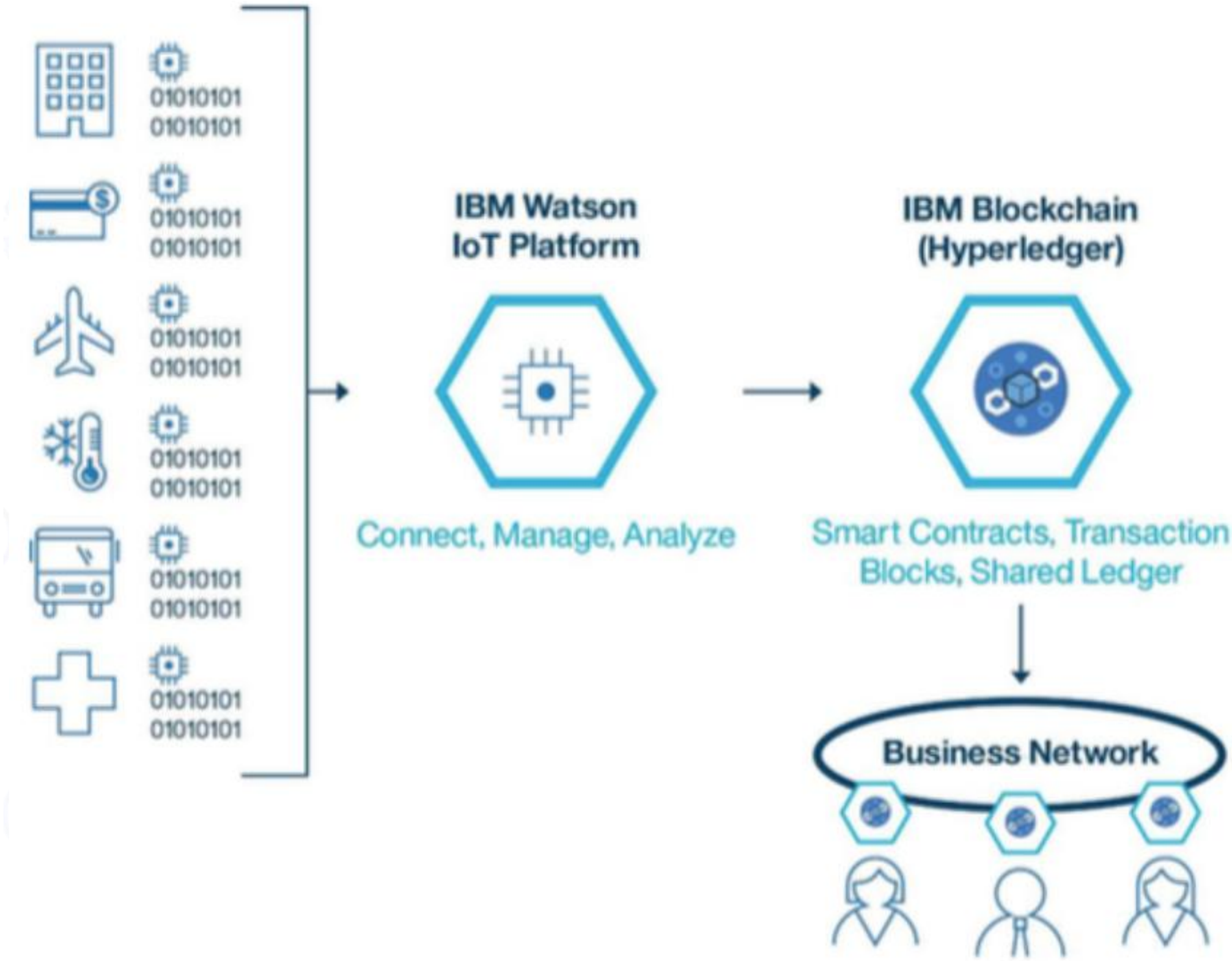

正如 IT 关注数据和连接向“智慧”边界设备的迁移，安全同样关心这种转变。毕竟，网络的扩展可能会提升 IT 效率、生产力并降低耗电量，但也给 CISO、CIO 和整个公司带来了安全挑战。很多公司因而寻求应用区块链来保护物联网及工业

物联网(IIoT)设备安全的方法——因为区块链技术可增强身份验证，改善数据溯源和流动性，并辅助记录管理。

## 6.2 改进机密性和数据完整性

尽管区块链最初创建时是在没有特定访问控制的机制下（由于其公开发布），但现在一些区块链实现解决了数据机密性和访问控制挑战。在当今数据极易被篡改或伪造的时代，这显然是一项重大挑战，但区块链数据的完全加密可确保未经授权的各方在传输过程中无法访问这些数据（中间人攻击几乎没有可能）。

此数据完整性扩展到物联网及工业物联网设备。例如，IBM 为其 Watson IoT 平台提供了一个选项，用于管理私有区块链分类账中的物联网数据，该分类账已集成到 Big Blue 的云服务中。爱立信的区块链数据完整性服务为在 GE 的 Predix PaaS 平台上工作的应用程序开发人员提供完全可审计，合规且值得信赖的数据。




# 6.3 保护隐私信息

像 Obsidian 这样的初创公司正在使用区块链来保护即时聊天和社交媒体上流转的隐私信息。与 WhatsApp 和 iMessage 之类 App 所用端到端加密不同，Obsidian 使用区块链来保护用户的元数据。因为元数据是账本中随机分发，不存在单一的收集点，所以不会被黑。

另外，据报道，美国国防部高级研究计划局(DARPA)正在尝试利用区块链创建外来攻击无法渗透的安全消息服务。随着区块链植根于经验证的安全通信，隐私消息安全领域将会愈加成熟。

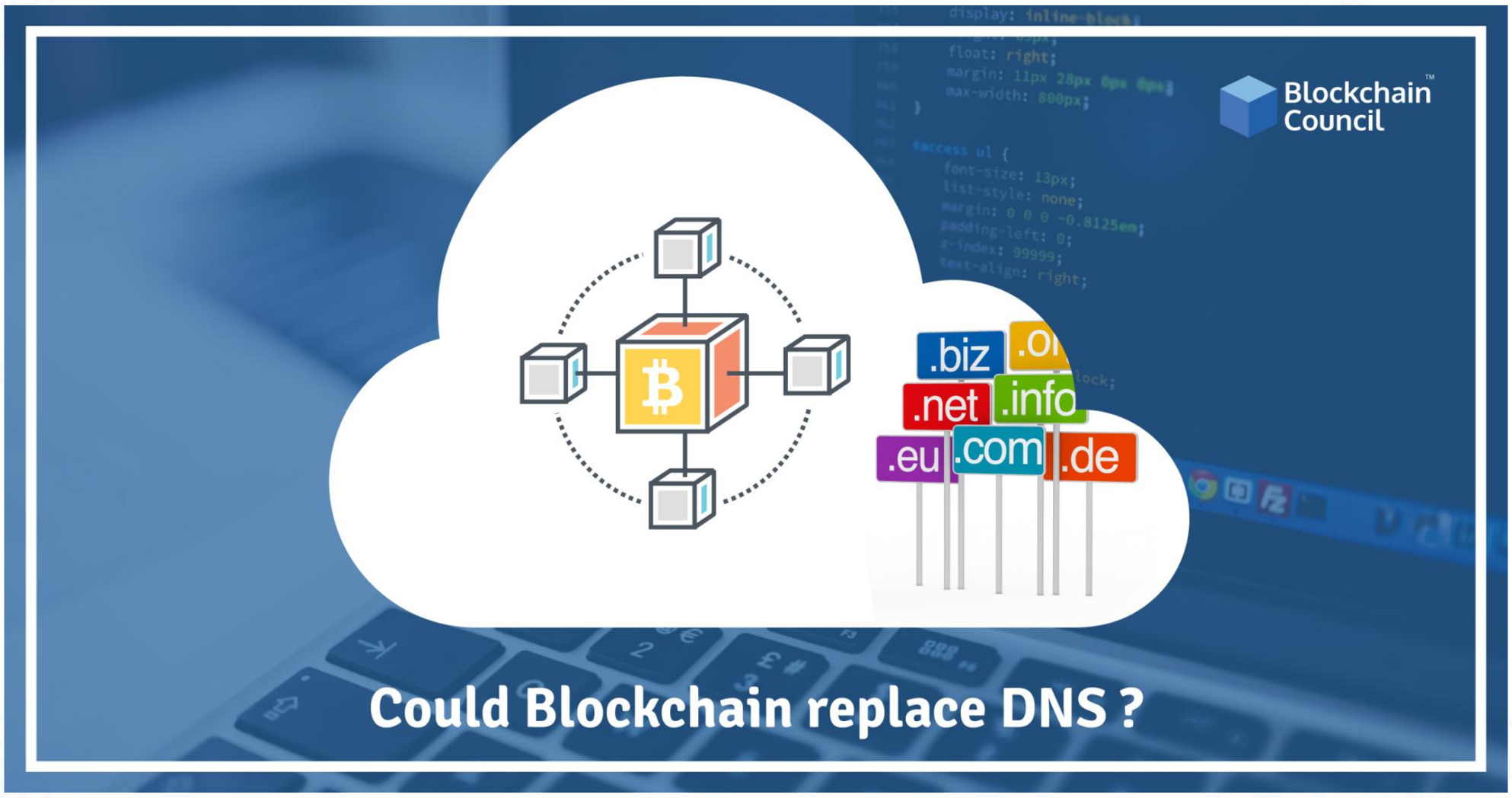
## 6.4 改进甚至替代公钥基础设施

公钥基础结构（PKI）是一种公钥加密技术，可以保护电子邮件，消息传递应用程序，网站和其他形式的通信。但是，大多数实现依赖于集中式第三方证书颁发机构（CA）来发布，撤销和存储密钥对，而这就给网络罪犯留下了窥探加密通信和假冒身份的机会。而在区块链上发布密钥则在理论上可杜绝虚假密钥传播，并可令应用具备验证通信对象身份的功能。

CertCoin 是基于区块链的 PKI 的首批实现之一。该项目完全摒弃了中央机构，并使用区块链作为域及其公钥的分布式账本。此外，CertCoin 还提供可审计的公共 PKI，并且不带单点故障。

目前，我们依赖 PKI 创建信任基础设施，但这往往是有漏洞的，尤其是网络罪犯如今也在创建自己的数字证书的情况下。依赖区块链技术，我们就可以用公民生成的身份来签名交易了。

# 6.5 更安全的 DNS



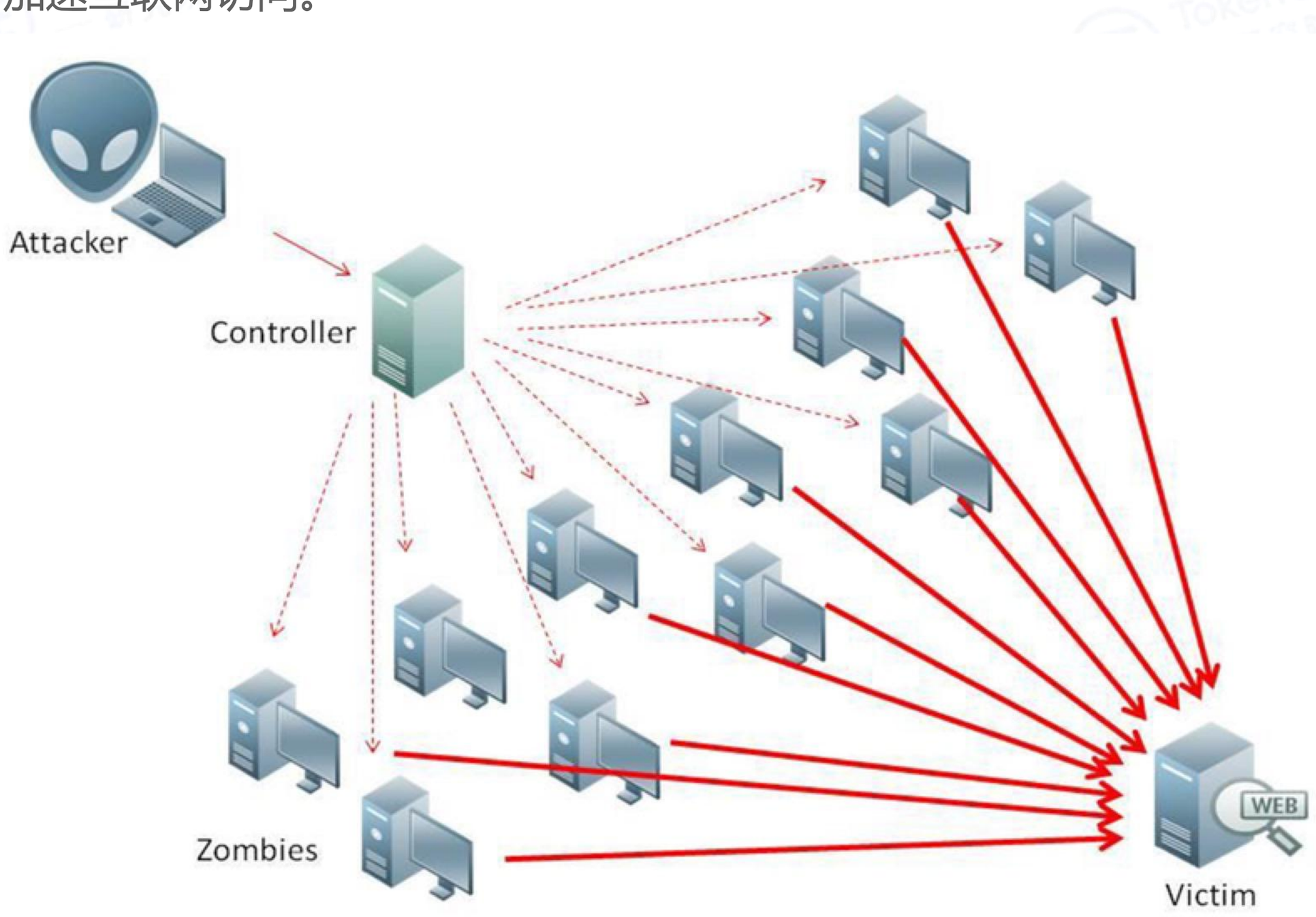

Mirai 僵尸网络证明了网络罪犯可以很容易地破坏关键互联网基础设施。攻击者只需搞定大型网站的域名系统(DNS)服务提供商，就可以切断推特、Netflix、PayPal 和其他服务的网络访问。而如果用区块链来存储 DNS 记录，理论上是可以通过去除该可攻击的单一目标而提升 DNS 安全。

Nebulis 是一个探索分布式 DNS 概念的新项目，理论上分布式 DNS 可以应付访问请求洪水，不会因响应过载而宕机。Nebulis 使用以太坊区块链和星际文件系统(IPFS)，还有 HTTP 的分布式替代协议，来注册并解析域名。DNS 之类互联网关键服务可被黑客利用来制造大规模掉线和攻击公司企业，因此使用区块链方法的可信 DNS 基础设施，将能大幅增强该互联网核心信任基础设施。

# 6.6 减少 DDoS 攻击

区块链初创公司 Gladius 宣称，其去中心化账本系统有助抵御 DDoS 攻击。在 DDoS 攻击峰值已超 100Gbps 的现在，这一断言还是很引人注目的。该公司称，其去中心化的解决方案可通过使客户接入附近防护资源池来提供更好的保护并加速客户内容，从而抵御 DDoS 攻击。

有趣的是，Gladius 宣称，该去中心化的网络能让用户出租空闲带宽赚点小钱，而这多余的带宽就被分配给了遭到 DDoS 攻击的网站节点以确保其能挺过攻击。而在不忙的时间里(没有 DDoS 攻击时)，Gladius 网络会扮演内容交付网络的角色，加速互联网访问。




DDoS 攻击形式

# 7.未来展望

目前区块链最核心的部分是通过数学算法的高难度机制，在现有的技术水平下保证了密钥的难以破解。不过量子计算机的技术也在研发过程中，并取得了一定的进展，对于此，部分数字货币从发布就确定了研发抗量子算法的大方向，像传统主流数字货币也可以选择在量子计算技术成熟后选择更换加密算法的方式去解决。

不过从最近频发的区块链安全事故来看，更多的安全问题是发生在用户、合约、平台层面，区块链的安全问题已经延伸到了传统的网络安全、基础设施、移动信息安全等问题。所以在谈及区块链安全的时候，不应该仅仅局限于区块链本身，它的使用者以及衍生的东西都需要我们的重点关注。

从目前区块链安全领域的布局来看，已经出现了像慢雾科技、Certik 这种专门服务于区块链安全的机构，也有像 360、知道创宇这种传统互联网安全的机构提供区块链安全服务。在未来随着区块链生态进一步扩大，会有更多与安全相关的问题亟待专业机构去解决，针对区块链安全所提供的服务也会更加的专业和细化。

总体来说，区块链技术和其安全性问题仍会持续很长一段时间，主要原因：其一，全新的解决方案会进一步加快区块链的安全重建，创新技术和服务得到认可，进一步增强产业活力，提升技术价值;其二：随着生产生活逐渐向数字化，网联化和智能化转型，许多全新的变革性技术(如区块链)所打造的安全生态体系和技术将成为大势所趋;其三，由新技术衍生的产品安全技术服务范畴更加宽泛，将会催生更加繁荣的安全服务市场。

# 8. 参考文献

[1] Bitcoin：A Peer-to-Peer Electronic Cash

http://www.bitcoin.org/bitcoin.pdf

[2] 区块链安全网：安全趋势

https://bcsec.org/analyse

[3] 腾讯安全《2018 上半年区块链安全报告》

https://slab.qq.com/news/authority/1754.html

[4] 白帽研究院《区块链安全报告》

https://bcsec.org/report

[5] Solidity Security: Comprehensive list of known attack vectors and common anti-patterns

https://blog.sigmaprime.io/solidity-security.html#dos

[6] Irreversible Transactions

https://en.bitcoin.it/wiki/Irreversible_Transactions

[7] Analysis of hashrate-based double-spending

https://bitcoil.co.il/Doublespend.pdf

[8] Solidity 合约中的整数安全问题——SMT BEC 合约整数溢出解析

http://www.freebuf.com/vuls/169741.html

[9] Decentralized Application Security Project (or DASP) Top 10 of 2018

https://www.dasp.co/

[10] Wikipedia：Sybil attack

https://en.wikipedia.org/wiki/Sybil_attack

[11] 6 use cases for blockchain in security

https://www.csoonline.com/article/3252213/security/6-use-cases-for-blockchain-in-security.html

[12] 区块链研习 | 区块链上的态势感知

https://www.leiphone.com/news/201808/SI388CNhjtTRtVxr.html

[13] 知道创宇：区块链安全风险白皮书

http://www.useit.com.cn/thread-19665-1-1.html

[14] 区块链安全 - DAO 攻击事件解析

https://blog.csdn.net/u011721501/article/details/79450122

[15] Ethereum Smart Contract Security Best Practices

https://consensys.github.io/smart-contract-best-practices/

TokenClub
研究院

TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。

扫码关注
TokenClub 研究院

扫码下载
TokenClub APP