区块链技术安全概述

国家互联网金融安全技术专家委员会
与上海圳链公司联合发布

目录 contents

国家互联网金融安全技术专家委员会持续跟踪区块链技术发展，对区块链安全、区块链+AI、区块链+供应链等领域进行深入调研，将推出系列报告。本报告聚焦于“区块链技术安全”，联合上海圳链公司共同推出，以期成为行业发展的研究依据。

一、 简述

区块链技术目前的发展方兴未艾，大多的技术和应用处于试验阶段，目前发生的安全事件多集中出现于加密资产相关领域，给用户造成了较大的经济损失，其安全问题日益受到行业关注。

同时区块链智能合约一旦在分布式、去中心化网络中部署，就难以变更，这种难以变更性一方面防止了数据操纵，建立起基于加密算法的信任机制。但另一方面，当区块链在面对安全攻击时，也就缺乏了有效的纠正机制，难以逆转。

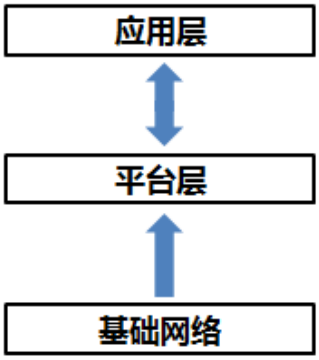

图 1 区块链应用架构

本文主要讨论了区块链的安全性问题，以及相应的解决方案和建议。 本文中，区块链应用从架构上分为三层：基础网络、平台层和应用层。三个层面相互影响，每一个环节出现的安全问题，都将给下个环节带来更多的安全问题。

因此，在进行区块链项目开发的过程中，从设计到实现，从验证到响应，不仅仅需要考虑到单个环节的安全性问题，也需要将其放入到整体的层面中去判断可能出现的风险点。

二、 基础网络安全风险

基础网络由数据层及网络层组成，是区块链的基础部分，该部分封装了区块链的底层数据，对区块链的数据采用非对称性加密，利用 P2P 网络并设置了传播、验证机制等，目前主要面临以下几类安全问题。

2.1 数据层：信息攻击与加密算法攻击

（1）数据区块信息攻击风险：一方面写入区块链后的信息很难删除，不法分子将某些有害信息、病毒特征码、淫秽信息等写入区块中，影响区块链生态环境。另一方面，大量的垃圾交易数据攻击会堵塞区块链，使得有效交易和信息迟迟无法被处理。

（2）加密算法安全风险：早年普遍使用的 SHA-1 于 2005 年 2 月被王小云、殷益群及于红波等人证明安全性不足，只需少于 2 的 69 次方的计算复杂度就能找到一组碰撞。此外 SHA-2 算法跟 SHA-1 基本相似，虽目前未出现有效攻击，但安全性已被严重质疑。其余的 SHA-224、SHA-256、SHA-384、SHA-512 等加密算法目前没有公开证据表明存在漏洞，但在量子计算高速发展的情况下，并不是无懈可击。目前针对加密算法进行攻击的方式主要有：穷举攻击、碰撞攻击、长度扩展攻击、后门攻击、量子攻击等。

2.2 网络层：节点传播与验证机制风险

（1）P2P 网络风险：区块链信息传播采用 P2P 的模式，节点之间的信息传播，会将包含自身 IP 地址的信息发送给相邻节点。由于节点安全性参差不

齐，较差的节点容易受到攻击，目前可进行攻击的方式有：日食攻击、窃听攻击、BGP 劫持攻击、节点客户端漏洞、拒绝服务（DDoS）攻击等。例如：2018 年 3 月以太坊网络爆出的“日食攻击”。

（2）广播机制风险：节点与节点之间相互链接，某节点将信息广播给其他节点，这些节点确认信息后再向更多的节点进行广播。在广播机制中常见的攻击方式有双花攻击及交易延展性攻击。双花攻击即同一笔加密资产被多次花费，当商家接受 0 确认交易付款时或者通过 51%算力攻击时这种情况较容易发生。交易延展性攻击也被称为可锻性，即同一个东西，本质没有变化，形状发生了改变，攻击者利用交易签名算法特征修改原交易 input 签名，生成一样的 input 和 output 的新交易，导致原有交易一定概率不被确认形成双花。

（3）验证机制风险：验证机制更新过程易出现验证绕过，一旦出现问题将导致数据混乱，而且会涉及到分叉问题，需要确保机制的严谨性。

2.3 解决方案与建议

基础网络作为区块链的底层，其安全性尤为重要。

- 与时俱进，关注技术安全方面的最新进展。在量子计算快速发展的情况下，加密系统只有不断研发更新才可防范黑客攻击。
- 接受专业的代码审计，了解相关安全编码规范。大多数区块链项目为了增加可信度和透明性，对其项目代码进行开源管理，然而这样也使得项目更易受到攻击，接受专业的代码审计及注重安全编码可以有效规避潜在的风险。

三、 平台层安全风险

平台层由共识层、激励层及合约层组成，是衔接基础网络与应用服务层的桥梁。该部分封装了网络节点的共识算法、发行机制、分配机制、脚本及智能合约等。

3.1 共识层：常见共识机制安全性对比

共识机制是对于一个时间窗口内的事务先后顺序达成共识的算法。区块链可支持不同的共识机制，目前存有的共识机制有 POW、POS、DPOS、POOl 验证池机制、BFT 等等。本文将介绍以下三种常见的共识机制攻击方式：

共识机制	内容	攻击方式
POW 工作量证明机制	节点通过计算随机哈希散列数值来争夺记账权	女巫攻击
POS 权益证明机制	根据节点拥有的通证比例及时间，依据算法降低挖矿难度，加快随机数的寻找速度	short-range 攻击、 Long-range 攻击、币龄累计攻击、预计算攻击、女巫攻击
DPOS 股份授权证明机制	全体节点投票选举一定数量的节点代表，由他们确认区块，维持系统秩序	Long-range 攻击、币龄累计攻击、女巫攻击

图 2 常见的共识机制攻击方式对比

3.2 激励层：发行与分配机制风险

（1）发行机制风险：目前暂无安全风险事件曝光，但不排除激励层发行机制中存在安全隐患。

（2）分配机制风险：大量小算力节点易集中加入矿池，对于去中心化趋势造成威胁。

3.3 合约层相关安全风险

合约层主要封装区块链的各类脚本、算法及智能合约。最初区块链只能用于交易，合约层的出现使得很多领域可以使用区块链技术。图灵完备的代表是以太坊，其合约层包括了以太坊虚拟机和智能合约两部分。目前合约层可能出现以下攻击对区块链的安全造成威胁：Solidity 漏洞、逃逸漏洞、短地址漏洞、堆栈溢出漏洞、可重入性攻击、交易顺序依赖攻击、时间戳依赖攻击、整数溢出攻击等。例如：2017 年 7 月 19 日在 github 上出现一个针对 VMware 虚拟机的逃逸 exploit 源码；2016 年 6 月 17 日，DAO 黑客利用重入性漏洞抽走了价值 5000 万美金的以太坊；2018 年 4 月 22 日，黑客利用机制漏洞，转出大量的通证，计算结果产生溢出，完成通证增发。BEC 无中生有出巨额通证，价值几乎归零。

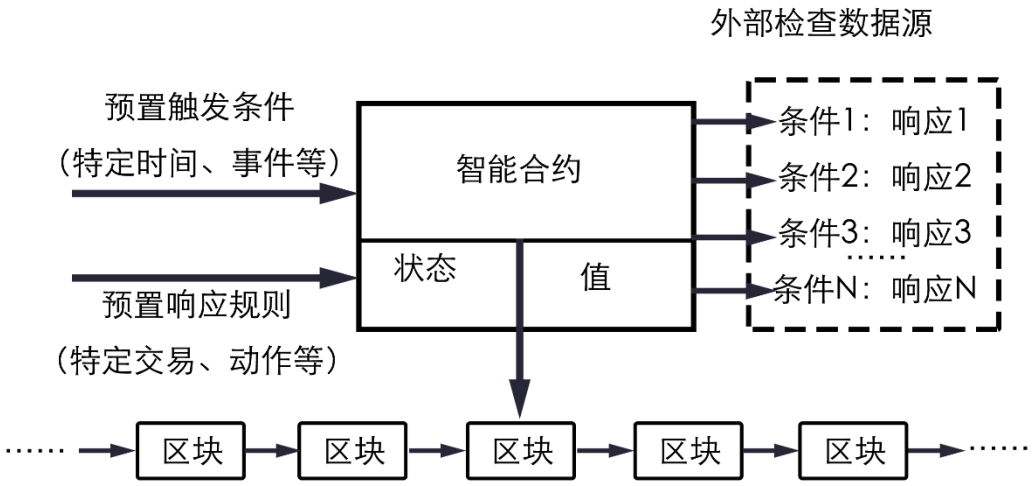

图 3 智能合约运作原理(来源：百度百科)

3.4 解决方案与建议

- 目前现有的共识机制均不是完美无缺的，需探求设计更安全性能更快的共识机制。
- 智能合约开发前需要对当下已经出现过的漏洞进行防范。

- 发布智能合约之前需要充分的进行安全测试。
- 关注相关情报，专业人员及时进行代码优化。
- 定期进行代码审计，包括但不限于：交易安全审查、访问控制审查等。
- 异常操作监控，监控已部署合约异常行为，降低损失。

四、 应用层安全风险

应用层作为区块链技术一个实际的落地场景，也是目前区块链产业的所有架构中受到安全性事件影响最多也是最频繁的一个层级。攻击目标主要集中在与加密资产相关的领域例如用户节点、数字资产钱包以及交易平台之中，每一次的安全事件所带来的实际损失可达千万至上亿美元。

4.1 节点常见安全问题

（1）傀儡网络是指恶意软件开发者或运营者通过感染受害者的系统和设备在对方不知情的情况下进行加密资产挖矿行为。

黑客主要通过在例如网页、游戏辅助程序、系统后台中安装木马程序的方式侵占用户的算力与电力，并用于采矿以谋求非法收益。美国哈佛大学与国家基金会的超级计算机在此前均受到过类似的攻击方式，国内也常常发生例如网页被串改或者应用程序被植入采矿木马的相关事件。

在当下采矿需要大量的计算能力的前提下，单一设备的算力已经无法满足采矿所需要的算力。于是攻击者扩大了攻击目标设备的范畴，尤其是易受到攻击的物联网设备成为了主要目标，这也形成更大规模的傀儡网络采矿，目前主

要的感染对象包括数字视频摄像机、路由器、监控摄像头、打印服务器、游戏机等。常见的攻击方式有：

- 跨站脚本攻击
- Microsoft 中远程执行代码的漏洞利用
- 命令缓冲区溢出漏洞利用
- SQL 注入
- BlackNurse 拒绝服务攻击

设备 OS/类型	安全事件
基于 Windows 操作系统	56231
Windows 8	28898
Windows 7	27857
小米路由器	17466
D-Link IPCam	6,843

图 4 2017 部分傀儡网络攻击事件统计（数据来源：TrendLabs）

（2）解决方案或建议

这些恶意软件可能会威胁系统的可用性、完整性和安全性，并使最终用户和企业面临信息窃取，劫持和感染其他恶意软件的风险。对于这些恶意软件没有一蹴而就的解决方案，但可以通过以下方式来减轻感染风险：

- 定期使用最新补丁更新设备有助于防止攻击者利用系统漏洞。
- 更改设备默认凭据并启用设备防火墙，尤其在使用家用路由器时。

- 禁用路由器中不必要的组件，也可重新配置路由器例如更改子网地址、使用随机 IP 地址、强制执行 SSL 等。
- 如果物联网家庭设备链接到移动设备，则仅通过官方 / 可信应用商店使用合法应用程序。
- 咨询 IT 管理员和安全专家，制定对策和监控流程，以预防或缓解高级威胁，例如采用应用程序白名单或类似安全机制。

4.2 加密资产钱包安全性对比

（1）区块链的钱包主要用于存储区块链资产的地址和私钥文件，目前根据使用场景的不同分为了不同类型的数字资产钱包，主要包括：

- 中心化钱包：使用用户名 / 密码进行登陆，可在多个链上交易多个通证。
- 多种类钱包：可通过相同的私钥保存不同链上的通证。
- 网络钱包：通过网络托管的链上钱包，有的需要将私钥存储在密码之后，有的则要求在对账户执行任何操作之前存储私钥并上传。
- 本地钱包：本地安装的软件，用于对特定区块链执行操作，私钥仍然需要存储在钱包可以访问的地方。
- 硬件钱包：冷钱包，存储在物理脱机设备中例如硬盘、USB，只在使用时连接网络。

（2） 目前影响安全的因素主要包括：

- 网络钓鱼：简单来讲为通过欺骗的方式获取访问账户所需信息。例如：通过邮件发送的需要输入私钥或账户密码的虚假链接。
- 恶意三方程序：来自非官方地址下载的有后台程序漏洞的钱包。

- 计算机黑客：跟踪计算机上执行的操作，输入密钥或密码将会被盗。
- 丢失密码 / 密钥：丢失存储的密钥、密码或助记词。

（3）不同的数字资产钱包安全性问题

	网络钓鱼	恶意三方程序	计算机黑客	丢失私钥
中心化钱包	x	x	x	
多种类钱包	x		x	x
网络钱包	x	x	x	x
本地钱包	x		x	x
硬件钱包	x			

图 5 各类型数字资产钱包安全性问题

有别于其他的应用程序，钱包因为各自用途、属性的不同，目前并无统一的解决方案，用户可以通过各自的适用性来判断相应适合的加密资产钱包，从用户的角度出发目前主要有以下几种拓展功能：

- 私钥控制：意味着可以随时使用其他软件获取私钥并访问数字资产，甚至可以直接在链上进行交互。
- 账户恢复：忘记密码或者丢失私钥时，可使用服务来恢复访问权限。
- 获取 AirDrop/Forks:当硬分叉发生或者通证被空投到另一个通证的持有者时，只能使用私钥获取这些新通证。
- 存储不同链上的通证：使用同一个账户存储不同链上的通证。

	私钥控制	账户恢复	访问 AirDrop/Forks	存储不同链上的通证
中心化钱包	不能	能	部分	能
多种类钱包	能	不能	部分	能
网络钱包	能	不能	能	不能
本地钱包	能	不能	能	不能
硬件钱包	能	能	能	部分

图 6 各类型数字资产钱包功能拓展

4.3 加密资产交易平台常见安全问题

（1）加密资产是数字经济中重要的组成部分，但针对加密资产交易平台展开的频繁网络攻击不断冲击着用户对于数字资产的信任。就在最近的几个月里，人们目睹了数起针对交易平台的攻击。例如日本的加密资产交易平台 Coincheck 于 2018 年 1 月被入侵，损失超过 5 亿美元。韩国交易平台 Coinrail 也证实它在 2018 年 6 月被黑客攻击，入侵损失达 3，690 万美元。

目前看来，加密资产交易平台主要有六类常见隐患和漏洞，即拒绝服务攻击、网络钓鱼事件，热钱包防护问题，内部攻击，软件漏洞，和交易可锻性。

- 拒绝服务攻击：攻击者通过拒绝服务攻击使得交易平台无法正常访问，也是目前最主要的针对交易平台的攻击方式。用户因为无法准确分辨攻击程度，往往会造成恐慌性的资产转移，从而给交易平台带来损失。
- 网络钓鱼事件：目前即使是最好的技术措施也无法保护加密资产交易平台免受网络钓鱼攻击。 欺诈者往往通过虚假域名或者仿冒页面的方式迷惑受害者，受害者如无法分辨交易平台的真实性便会遭受资产上的损失。

- 热钱包防护问题：许多交易平台使用单个私钥来保护热钱包，如果犯罪分子可以访问单个私钥，他们将能够破解与私钥相关的热钱包。 私钥攻击的典型例子是 2017 年首尔交易所 Yapizon 的攻击，攻击者一年内前后两次对交易平台发起了针对平台上热钱包的盗取，总共造成了交易平台近 50%的资产损失，并最终导致了交易平台的破产。
- 内部攻击：由于没有完善的风险隔离措施或对于员工权限监督不力，导致了部分拥有平台操作权限的员工利用内部信任监守自盗。例如 2016 年交易平台 ShapeShift 发生的员工盗取 BTC 事件，其通过私下盗取和将敏感信息转卖给其余人员的方式前后给交易平台造成了 23 万美元的损失。
- 软件漏洞：包括单点登陆漏洞、oAuth 协议漏洞等。各国都有法律要求银行或其他金融机构实施信息安全措施，以保护客户的存款。但是，由于区块链领域还处于起步阶段，目前缺少适用于加密资产的此类规范。 因此，许多交易平台在缺乏安全规范约束的条件下，存在大量漏洞并非偶然。
- 交易可锻性：区块链技术的支持者常常认为区块链交易是高度安全的，因为它们被记录在据称不可更改的记录上。但是每个交易都需有相应签名，而在交易最终确认之前，记录是可以被暂时伪造的。“Mt.Gox 事件“是加密资产历史上最大的攻击之一，共造成了 4.73 亿美元的损失，而这次攻击事件便是由黑客在初始交易发布之前向公共帐本提交代码更改进行的。

（2）解决方案与建议

- 在技术开发方面持续的投入，抵御日益增长的黑客攻击，切实的增强系统的安全性。

- 确保员工保护安装在专业工作计算机或个人计算机上软件应用程序相关的登录凭据，并完善安全培训，提高安全意识。
- 定期的安全测试，建立完善的应急相应机制。
- 网络安全隔离，谨慎进行服务端口开放。
- 选择具备完善防护的能力的服务供应商。
- 行业需要统一的治理机制，引入第三方监管与合作，在出现问题时及时与外部协同工作。

五、 小结

以上内容概述了区块链三个架构层中可能存在的安全问题。总体来说，一是在架构设计上，由于区块链应用具有高度自治特性，智能合约一旦运行就无法逆转，因此初期的安全设计规范尤显重要。二是在具体开发阶段，目前部分区块链开发者的代码质量、开发工具和应用平台的成熟度都需要进行不断完善与提升。三是区块链问题外延方面，鉴于安全问题始终是非静态的，关注区块链底层技术的安全问题同时，区块链安全问题同样外延到了传统的个人信息安全保护、基础设施安全、网络安全等领域中，无论是在区块链概念上,还是在实际应用层面上,都需要长期有效的校正机制。

国家互联网金融安全技术专家委员会将持续跟踪该行业发展，未来将陆续发布更多相关领域研究报告。

关于圳链科技

上海圳链网络科技有限公司致力于打造一个专业的区块链领域项目评估机构。公司设有区块链研究院，聚集了一批具有丰富行业经验的区块链研究人员和技术人员，从区块链技术和商业系统等多方位视角出发，通过量化审核指标，深度剖析项目内核，力求对区块链项目进行多维度，综合性的审慎考察，形成具有行业权威性的项目评估报告，共同推动区块链行业的发展。

专业·客观·全面

更多资料，社区交流

扫一扫添加微信号